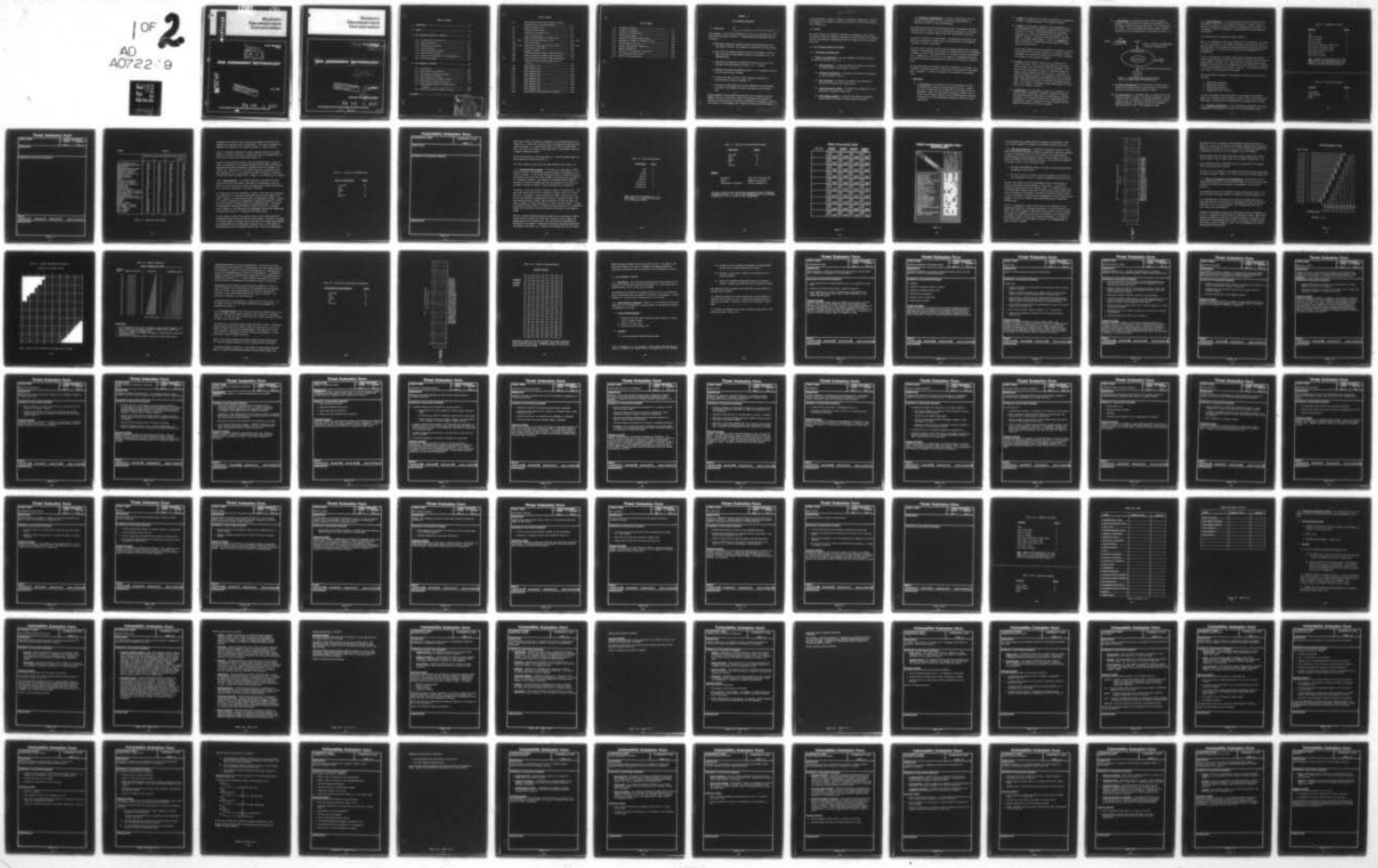
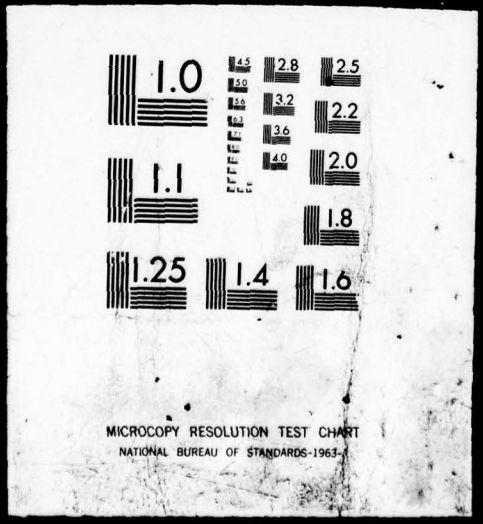
AD-A072 249 SYSTEM DEVELOPMENT CORP MCLEAN VA F/G 9/2
RISK ASSESSMENT METHODOLOGY.(U)
JUL 79
UNCLASSIFIED SDC-TM-WD-7999/001/03 N000173-78-C-0455
NL

1 OF 2
AD
A072219





LEVEL

System Development Corporation

TM-WD-7999/001/03
FINAL

RISK ASSESSMENT METHODOLOGY

JULY, 1979

System Development Corporation

(14) SDC-TM-WD-7999/001/03

(9) FINAL rept.

(6) # RISK ASSESSMENT METHODOLOGY.

(12) 183p.

(11) JUL[illegible]1979

(15) CONTRACT NO.: N00173-78-C-0455

339 860

JOB

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

APPENDIX ___

RISK ASSESSMENT METHODOLOGY

1.1 INTRODUCTION

This report treats risk assessment as

Risk assessment is an organized examination of events and conditions that could harm a Navy ADP system or facility. A comprehensive risk assessment does the following:

- Identifies conditions or potential events that threaten harm to the ADP system or facility, and evaluates the seriousness of these threats.
- Identifies and evaluates conditions within the ADP system or facility that could allow the ADP system or facility to be damaged, i.e., its vulnerabilities;
- Identifies and evaluates the properties and importance of all of the resources of the ADP system or facility, i.e., its assets;
- Estimates the Annual Loss Expectancy (ALE) of the ADP system or facility from the threats being realized;
- Estimates the level of risk to which classified, sensitive, or mission-essential assets are exposed; and
- Identifies the most dangerous or costly weaknesses of the ADP system or facility, and recommends the most cost-effective way to remedy them.

A risk assessment involves a detailed examination of the threats to the ADP system or facility; the missions, assets, and procedures of the system or facility; and the operational and security weaknesses of the system or facility. To be useful, a risk assessment must consider the current status and mission

(cont on p. 2)

(cont fr p 1)

of the ADP system or facility. Changes in the mission, configuration, location, or procedures of the system or facility are cause for a review of the existing risk assessment.

1.2 PURPOSE

The primary purpose for conducting a periodic risk assessment is to evaluate the exposure of Navy ADP systems or facilities to various threats and to identify the most cost-effective countermeasures that will reduce the risk to an acceptable level.

1.3 RISK ASSESSMENT METHODOLOGY OVERVIEW

1.3.1 Introduction and Definitions.

a. Format of the Methodology. The risk assessment methodology consists of the following six major activities:

(1) Threat Evaluation. To identify threats and estimate the frequency of attacks against the ADP system or facility.

(2) Vulnerability Evaluation. To identify and evaluate the weaknesses of the ADP system or facility.

(3) Asset Evaluation. To identify the assets of the ADP system or facility and determine their value and use.

(4) Threat/Vulnerability Merger. To estimate the susceptibility of an ADP system or facility to each threat.

(5) Asset Exposure Analysis. To quantify the effects of successful attacks against the assets of the ADP system or facility.

(6) Selection of Countermeasures. To select countermeasures that will reduce the asset exposure and to re-evaluate the asset exposure to determine the effect of those countermeasures.

The first three activities are data gathering tasks. This appendix provides forms and tables to assist in the identification and evaluation of the threats, vulnerabilities, and assets common to most Navy ADP systems or facilities.

The next two activities are computational. This appendix also provides forms and tables to compute the current level of security based on the information collected in the first three tasks.

The final activity involves gathering data, performing computations, and making judgments. Countermeasures are considered for implementation and are recommended if mandated by policy, cost-effectiveness, or the need to reduce an unacceptable risk. Judgment plays a major role in the selection of countermeasures because the number of possible countermeasures and combinations prohibits an exhaustive trial.

The individual tasks are described in detail in paragraphs 1.3.2 through 1.3.7. Paragraph 1.4 provides step-by-step instructions for performing the risk assessment. (Attachment _-1 contains an example of the completed risk assessment forms.)

b. Definitions.

(1) An ADP facility is a functional unit that encompasses one or more ADP systems and provides all required support functions. Support functions include power and environmental control systems as well as maintenance, guard, and other support personnel as needed. An ADP facility may be fixed or mobile; it may be organizationally dedicated or shared; and it may be intended for peacetime, crisis, or wartime applications.

(2) An asset of an ADP system or facility is any physical, informational, software, or personnel resource of the system or facility.

(3) A threat to an ADP system or facility is any circumstance or set of circumstances with the potential to cause harm to the system or facility in the form of unauthorized destruction, disclosure, modification, or denial of service of any of the assets of the system or facility. A threat may arise from natural, malicious-human, or accidental-human causes. A threat is a potential for harm; the presence of a threat does not mean that it will necessarily cause actual harm.

Threats exist because of the very existence of the system or facility and not because of any specific weakness of the system or facility. For example, the threat of fire exists at all facilities, regardless of the amount of fire protection available.

(4) An attack on an ADP system or facility is the realization of a threat. How often a threat is acted upon depends on such factors as the location, type, and value of information processed. Thus, short of moving the system or facility, or radically changing its mission, there is usually no way that the level of protection can affect the frequency of attack. The exceptions to this are certain human threats where effective security measures can have a deterrent effect. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends upon the vulnerability of the system or facility.

(5) A vulnerability of an ADP system or facility is a weakness in its physical layout, organization, procedures, hardware, or software that may be exploited to cause harm to the ADP system or facility. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that will allow the ADP system or facility to be harmed.

(6) A countermeasure is any protective action, device, procedure, technique, or other measure that reduces the vulnerability of an ADP system or facility to successful attack, i.e., the realization of a threat. (The relationships among assets, threats, attacks, vulnerabilities and countermeasures are illustrated in Figure _-1.)

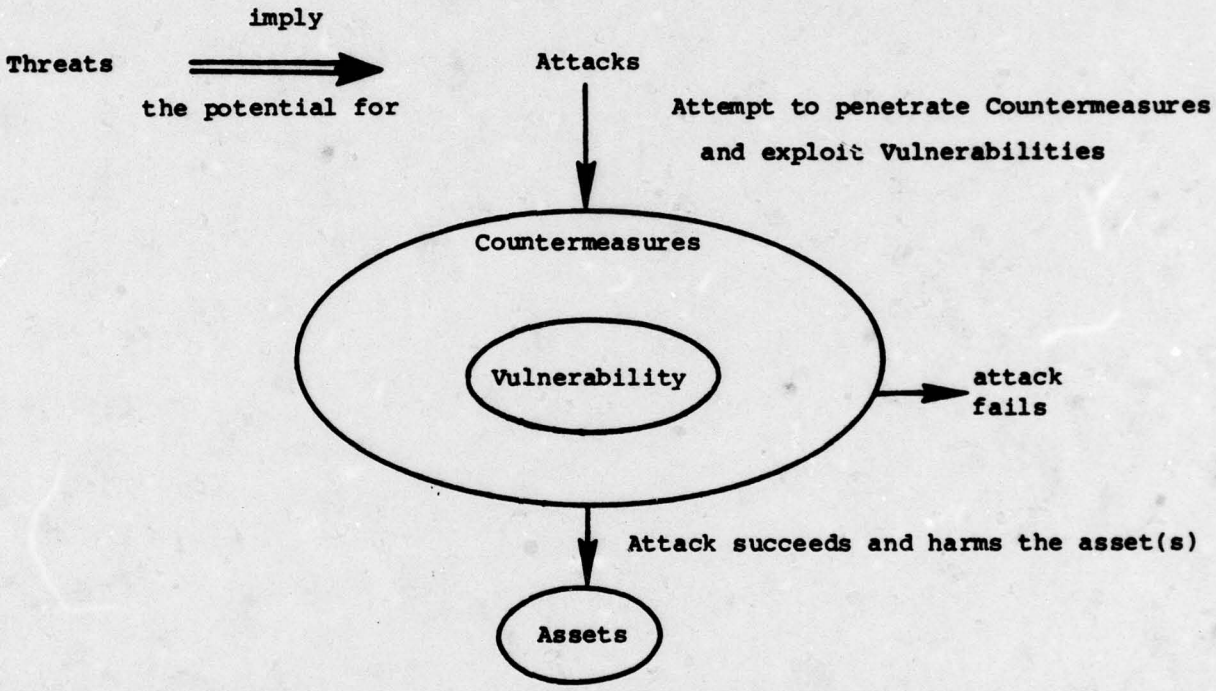


Figure _-1. Relationship between Assets, Threats, Attacks, Vulnerabilities, and Countermeasures

(7) The Annual Loss Expectancy of an ADP system or facility is the average yearly financial cost of the harm done to the system or facility by successful attacks against its assets.

(8) The level of risk for a particular asset is a measure of how frequently the asset is likely to be attacked successfully. Whether a level of risk is acceptable or unacceptable will be a policy or subjective decision. Only assets that can not be assigned a dollar value have a level of risk computed for them.

1.3.2 Threat Evaluation. In a threat evaluation, all of the threats to the ADP system or facility are to be identified and rated. A threat is rated in terms of the frequency of attacks against the system based on the threat. For the purposes of this risk assessment, a coarse estimate of these frequencies is sufficient.

The ratings that can be selected are shown in Table _-1.

Often, it is impossible to make even an estimate with much accuracy. To account for this, the precision of the frequency estimates is qualified using Table _-2. This can later be used to perform a worst-case analysis of how large the Annual Loss Expectancy or risk level could be, based upon the inadequacies of the available data.

To aid in the evaluation of threats, several generic threats to ADP systems and facilities have been identified and described on preprinted threat evaluation forms, Figures _-7 through _-35. These forms are to be used to record threat frequency. The threat list is not exhaustive and should be added to if necessary to cover threats peculiar to the system or facility. A blank Threat Evaluation Form, Figure _-2, is provided for this purpose.

Threats may affect the assets of the ADP system or facility in one or more of four ways:

1. Unauthorized Destruction
2. Unauthorized Disclosure
3. Unauthorized Modification
4. Unauthorized Denial of Service

For each of the generic threats identified in this appendix, the potential impact of the threat has been identified in Figure _-3 and on the threat evaluation forms. The impacts must be identified for any threats that are added.

1.3.3 Vulnerability Evaluation. In the vulnerability evaluation, all of the weaknesses of the ADP system or facility are to be identified and rated. A

Table _-1. Frequency of Attacks

Frequency	Rating
Never	0
Once in 300 years	1
Once in 30 years	2
Once in 3 years	3
Once every 4 months or 3 times a year	4
Once a week or 52 times a year	5
Once a day or 365 times a year	6
Once every 2 hours	7
Once every 15 minutes	8

Note: Ratings may be modified by $^{+}$ for "more often than" or $^{-}$ for "less often than." For example, 3^{+} is more often than every 3 years and 3^{-} is less often than every 3 years.

Table _-2. Precision of Estimate

Precision	Rating
Very Precise	V
Fairly Precise	F
Rough	R

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)

DESCRIPTION

EXAMPLES & EVALUATION GUIDANCE

IMPACT

DESTRUCTION ☐ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-2

THREATS	IMPACTS			
	Destruction	Disclosure	Modification	Denial of Service
Post Employment Access	Yes	Yes	Yes	Yes
Disgruntled Employee Access	Yes	Yes	Yes	Yes
Agent Access	Yes	Yes	Yes	Yes
Uncleared Personnel Access	Yes	Yes	Yes	Yes
Emanations (Unintended)	No	Yes	No	No
Emanations (Covert)	No	Yes	No	No
Emanations (Interference)	Yes	No	Yes	Yes
Improper Marking	No	Yes	No	No
Improper Handling	No	Yes	No	No
Fraud	No	Yes	Yes	No
Alteration of Software	Yes	Yes	Yes	Yes
Alteration of Hardware	Yes	Yes	No	Yes
Disclosure of Information	No	Yes	No	No
Physical Theft	Yes	Yes	No	Yes
Eavesdropping	No	Yes	No	No
Misuse of Resources	No	Yes	No	Yes
Intentional Denial (Software)	No	No	No	Yes
Intentional Denial (Hardware)	No	No	No	Yes
Power Instability	Yes	No	Yes	Yes
Telecommunications Failure	No	No	No	Yes
Environmental Control Failure	No	No	No	Yes
Sabotage	Yes	No	No	Yes
Weather	Yes	No	No	Yes
Natural Disaster	Yes	No	No	Yes
Water Damage - Internal	Yes	No	No	Yes
Water Damage - External	Yes	No	No	Yes
Fire - Internal	Yes	No	No	Yes
Fire - External	Yes	No	No	Yes
Enemy Overrun	Yes	Yes	No	Yes

Figure _-3. Threats and Their Impact

vulnerability is rated in terms of how weak the system or facility is with respect to the particular type of vulnerability. The level of vulnerability represents the inability of the system or facility to resist an attack.

Since it is generally infeasible to assign a numerical value to the vulnerability of a system or facility in a particular area, the vulnerabilities are rated using the descriptive terms found in Table _-3.

To aid in the evaluation of system or facility vulnerabilities, a number of common vulnerabilities of ADP systems and facilities have been identified and described on preprinted vulnerability evaluation forms, as in Figures _-38 through _-62. These forms are to be used to record the vulnerability level. The vulnerability list is not exhaustive and should be added to if necessary. A blank Vulnerability Evaluation Form , Figure _-4, is provided for this purpose.

1.3.4. Asset Evaluation. In the asset evaluation, each asset of the ADP system or facility is identified. Each asset is then assigned a value for each of the four ways in which threats can impact assets (unauthorized destruction, disclosure, modification, and denial of service).

In a broad sense, the value assigned to an asset in each impact area represents the importance of not allowing the particular type of harm to happen to the asset. Ideally, all values should be able to be expressed in dollars. However, it is often the case that the consequences of something happening to an asset can not be assigned a financial cost in any reasonable manner. For example, the compromise of classified information, denial of service of a guidance control computer, or the destruction of irreplaceable records have consequences far beyond any financial cost associated with these actions.

For this reason, an asset can be rated as either or both "dollar-valued" or "non-dollar-valued" for each of the four threat impacts. An asset is considered to be dollar-valued in an impact area if the result of the asset being affected in the particular way can be assigned a financial value. If the result of being affected can not be assigned a dollar value, or there are consequences

Table _-3. Ratings for Vulnerabilities

Level of Vulnerability	Rating
Very High	VH
High	H
Medium	M
Low	L
Very Low	VL

Vulnerability Evaluation Form

VULNERABILITY NAME	VULNERABILITY LEVEL (TABLE __-3)
DESCRIPTION	
EXAMPLES & EVALUATION GUIDANCE	
JUSTIFICATION	

Figure _-4

other than financial, the asset is considered to be non-dollar-valued in the impact area. An asset can be dollar-valued in one impact area and non-dollar-valued in another; or it may have both types of values in the same impact area. The latter will be true in many cases where a single asset is used for a number of different purposes.

Dollar-valued assets are rated using Table _-4. Non-dollar-valued assets are given subjective ratings using Table _-5

This data collection is done using the Asset Evaluation Form (Figure _-5).

1.3.5 Threat/Vulnerability Merger. If a threat is to cause harm to an ADP system or facility, the threat must be able to exploit a vulnerability in the system or facility. In the threat/vunerability merger, an estimate is made of the frequency with which each threat succeeds in exploiting each vulnerability of the system or facility. The frequency of successful attacks against a particular vulnerability depends upon both the frequency of all attacks and the degree to which the system or facility possesses the vulnerability.

In general, a threat can attempt to exploit a number of vulnerabilities. However, some threats clearly have no potential to exploit some of the vulnerabilities. For example, a person attempting to commit a fraud would not be able to take advantage of inadequacies in the air conditioning system. Also, some threats are able to exploit some vulnerability to cause one impact and unable to exploit the same vulnerability to cause a different impact. A person could exploit gaining access to information through penetration of the operating system, but this would not lead to the physical destruction of the computer itself.

There is a separate Threat/Vulnerability Merger Form for each type of impact. On each form, the threats that could have a particular type of impact are matched against all vulnerabilities. For the threats and vulnerabilities identified in this chapter, inappropriate combinations have been removed from consideration (see Figure _-6). Threats and vulnerabilities that are unique

Table _-4. Dollar-Valued Assets

Dollar Value	Rating
$10	1
$100	2
$1,000	3
$10,000	4
$100,000	5
$1,000,000	6
$10,000,000	7
$100,000,000	8

Note: Ratings may be modified by a + or -. For example, a 3+ is more than $1,000 and a 4- is less than $10,000.

Table _-5. Ratings for Non-Dollar-Valued Assets

Value Level	Rating
Very High	VH
High	H
Medium	M
Low	L
Very Low	VL

Example:

Top Secret	High (H) to Very High (VH)
Secret	Medium (M) to High (H)
Confidential, Privacy Act	Low (L) to Medium (M)

All other non-dollar-valued assets such as sensitive business information, proprietary software, etc., can be rated subjectively by the risk assessor at Medium (M), Low (L), or Very Low (VL) as applicable.

ASSET EVALUATION FORM

ASSET NAME	UNAUTHORIZED DESTRUCTION	UNAUTHORIZED DISCLOSURE	UNAUTHORIZED MODIFICATION	UNAUTHORIZED DENIAL OF SERVICE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE

Figure _-5

THREAT/VULNERABILITY MERGER FORM—MODIFICATION

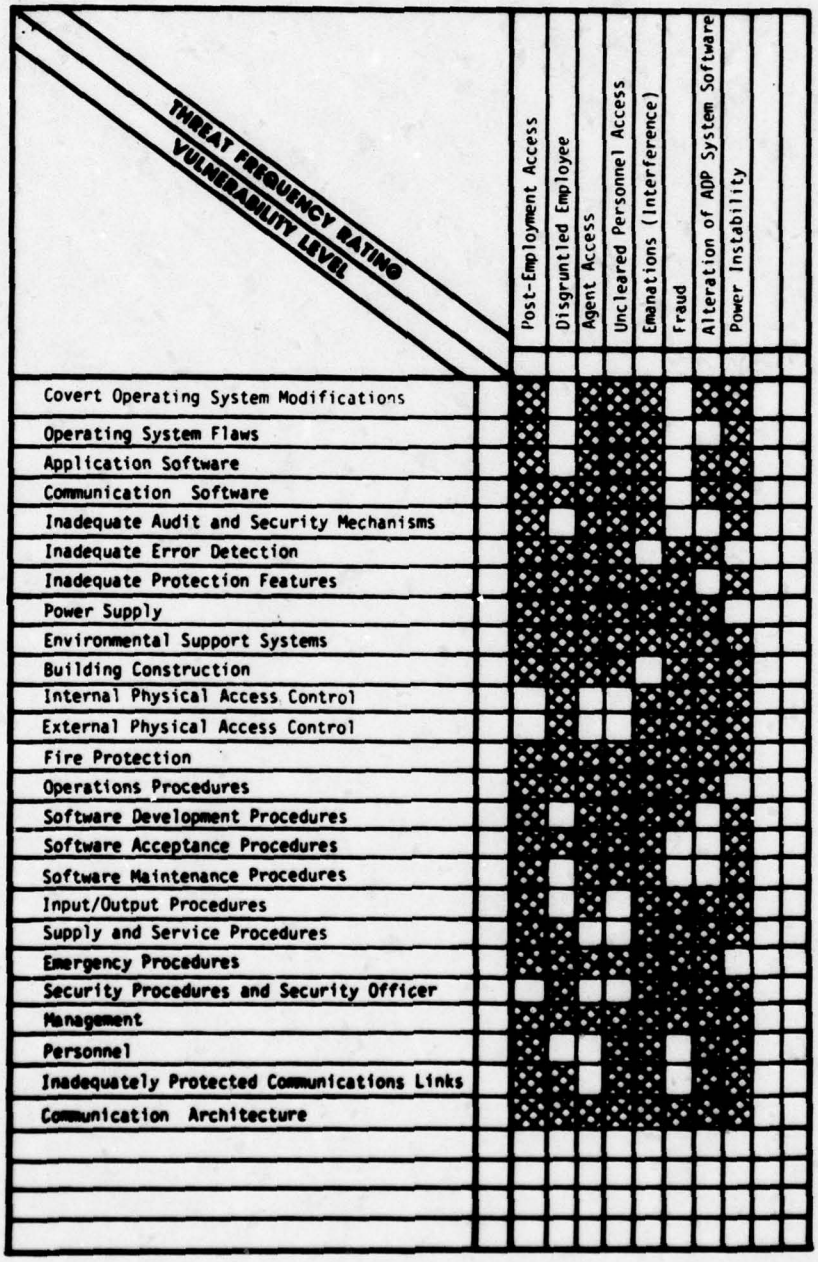


Figure _-6

to an ADP system can be added and must be included in the procedure. Table _-6 is used to estimate the frequency of successful attacks for each pair.

1.3.6 Asset Exposure Analysis. A threat that successfully exploits a vulnerability can harm the ADP system or facility by destroying, disclosing, modifying or denying the service of any or all of the assets of the system facility. The asset exposure analysis measures the impact that the threats are likely to have on the assets of the ADP system or facility. This impact can be measured in two ways for each of the four types of harm.

1. The Annual Loss Expectancy (ALE) for an asset if the harm has financial consequences (dollar-valued).

2. The level of risk for an asset if the main consequence of the harm can not be measured in terms of a financial consequence (non-dollar-valued).

The ALE is the measure of the long-term expected cost to the ADP system or facility from security events averaged on a yearly basis. The ALE is an estimate of average yearly cost to replace, repair, or reconstruct assets, and the average yearly financial penalties or losses resulting from delayed processing or disclosures of information. The ALE is the preferred measure because it gives a solid basis for justifying the implementation of money-saving countermeasures. It is also a standard, easily understandable way of quantifying probable loses.

Often it is impossible to assign a dollar value to the conseqences of the unauthorized destruction, disclosure, modification, or denial of service of an asset. This is not because of insufficient data upon which to make a judgment, but because the consequences are so great, irreversible, or far-reaching that any attempt to attach a dollar value to them is meaningless. For these non-dollar-valued assets, the best measure of security is the level of risk to which the asset is exposed.

Table _-6. Estimation of Number of Successful Attacks

Vulnerability Level:	Threat Rating																							
	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8	8⁺
VL	0	0	0	0	0	0	0	0	0	0	0	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1	1	1
L	0	0	0	0	1⁻	1⁻	1	1⁺	1⁺	1⁺	2⁻	2⁻	2⁻	2	2	2	2⁺	2⁺	2⁺	2⁺	3⁻	3⁻	3⁻	3
M	0	1⁻	1⁻	1	1	1⁺	2⁻	2	2	2	2⁺	2⁺	3⁻	3⁻	3⁻	3	3	3⁺	4⁻	4	4⁺	5⁻	5	5
H	1⁻	1	1⁺	2⁻	2	2	2⁺	3⁻	3	3⁺	4⁻	4	4	4⁺	5	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻
VH	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8	8⁺

Instructions: Ignore the precision portion of the threat rating. Locate the row and column marked with the appropriate vulnerability level and threat rating. The rating for the estimate of the number of times that the threat exploits the vulnerability is found at the intersection of the row and column.

The level of risk is an estimate of how frequently the asset in question is likely to be affected in the way that could produce unquantifiable consequences. Whether or not the level of risk to which an asset is exposed is acceptable must be detemined by either policy or the judgement of the risk assessor.

ALEs are computed for individual assets and the entire system; broken down by type of threat or over all impact areas; and by separate vulnerability. The

latter breakdown allows the weaknesses which are responsible for the greatest loss to be identified and corrected.

The level of risk is computed in each impact area for any individual assets where the measure is needed. Tables _-7, _-8, and _-9 are used for these computations.

1.3.7 Selection and Application of Countermeasures. Beyond giving a view of current security and risks at an ADP system or facility, a risk analysis provides a method for determining which potential countermeasure (if any) would be desirable.

Countermeasures should only be applied to achieve some specific benefit. This benefit could be a savings of money or a reduction of some unacceptable risk.

For a countermeasure to save money over the life of a system, the amount of money saved over all the years that the countermeasure is used must exceed the installation cost for the countermeaure. Any countermeasure where this is true is said to be cost-effective.

Sometimes, countermeasures that are not cost-effective must be implemented, if the risk of compromising classified data is exceptionally large. These countermeasures are required if Top Secret or Secret information is processed. Non-cost-effective countermeasures may also need to be applied to reduce unacceptable risks in cases not covered by policy. The risk assessment will help to identify these countermeasures.

ADDING FREQUENCY RATINGS

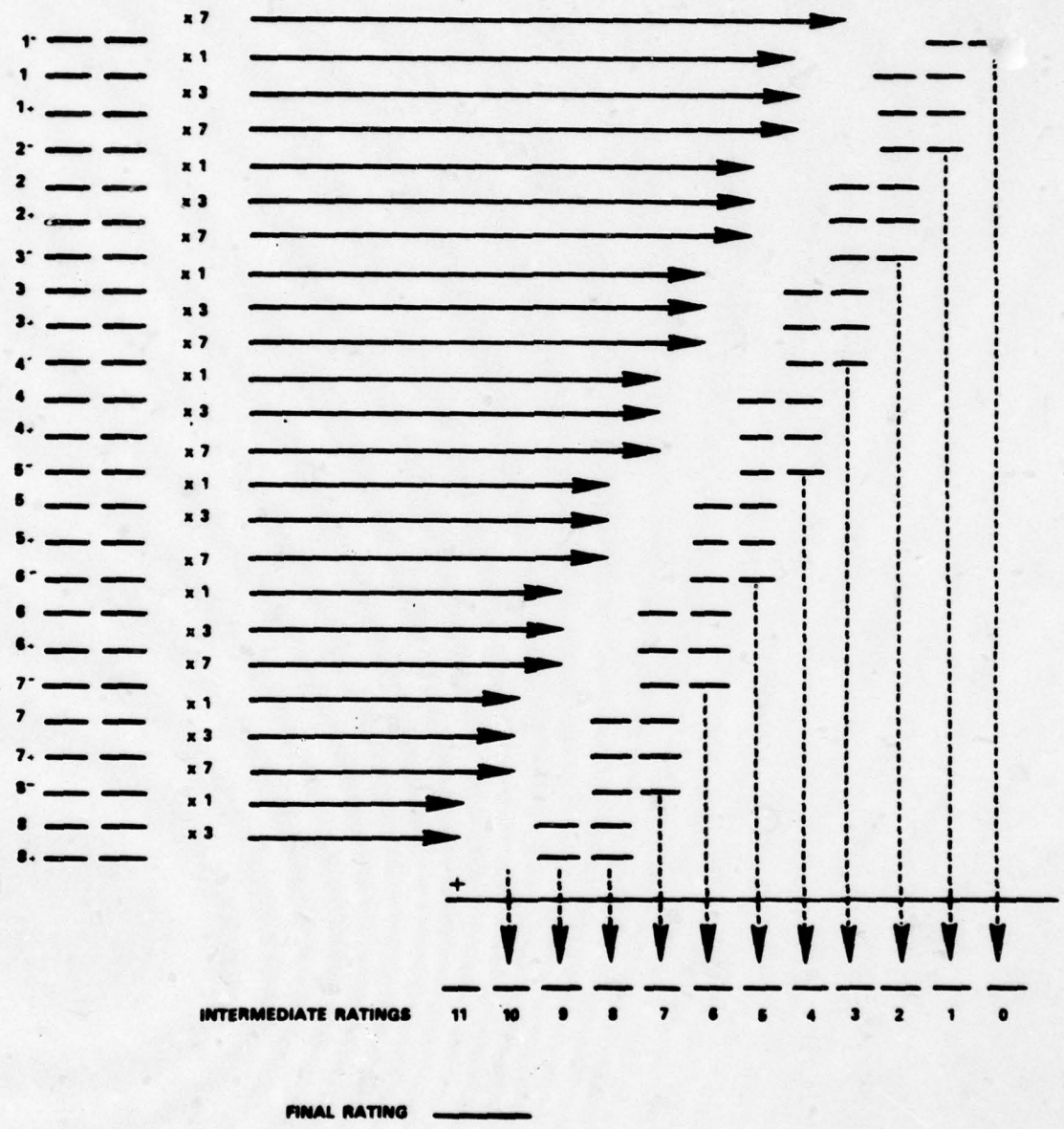


Table _-7

Table _-8. Average Asset Exposure Computation

Frequency of Successful Attacks

	1^-	1	1^+	2^-	2	2^+	3^-	3	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+
1^-										1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+
1									1	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6
1^+									1	1^+	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6
2^-							1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+	6^-	6^-	6^+
2						1	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7
2^+						1	1^+	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6	6^+	6^+	7
3^-				1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+	6^-	6^-	6^+	7^-	7^-	7^+
3			1	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8
3^+			1	1^+	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6	6^+	6^+	7	7^+	7^+	8
4^-	1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+	6^-	6^-	6^+	7^-	7^-	7^+	8^-	8^-	8^+
4	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9
4^+	1^+	2^-	2	2^+	3^-	3	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9
5^-	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6	6^+	6^+	7	7^+	7^+	8	8^+	8^+	9	9^+
5	2	3^-	3	3	4^-	4	4	5^-	5	5	6^-	6	6	7^-	7	7	8^-	8	8	9^-	9	9	10^-	10
5^+	2^+	3^-	3^+	3^+	4^-	4^+	4^+	5^-	5^+	5^+	6^-	6^+	6^+	7^-	7^+	7^+	8^-	8^+	8^+	9^-	9^+	9^+	10^-	10^+
6^-	3^-	3	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+
6	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9	9	9^+	10	10	10^+	
6^+	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+		
7^-	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+			
7	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9	9	9^+	10	10	10^+				
7^+	4^+	5^-	5^+	5^+	6^-	6^+	6^+	7^-	7^+	7^+	8^-	8^+	8^+	9^-	9^+	9^+	10^-	10^+	10^+					
8^-	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+						
8	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9	9	9^+	10	10	10^+							
8^+	5^+	6^-	6^+	6^+	7^-	7^+	7^+	8^-	8^+	8^+	9^-	9^+	9^+	10^-	10^+	10^+								

Note: Ignore precision estimates for average exposure ratings.

Table _-9. Exposure Computation

Asset or Vulnerability Name: _____

Exposure Value	Number of Ratings:	x	Multiplier	=	Intermediate Value
1-	_____	x	7	=	_ _ _
1	_____	x	10	=	_,_ _ 0
1+	_____	x	30	=	_,_ _ 0
2-	_____	x	70	=	_,_ _ 0
2	_____	x	100	=	_ _,_ 0 0
2+	_____	x	300	=	_ _,_ 0 0
3-	_____	x	700	=	_ _,_ 0 0
3	_____	x	1,000	=	_ _ _,0 0 0
3+	_____	x	3,000	=	_ _ _,0 0 0
4-	_____	x	7,000	=	_ _ _,0 0 0
4	_____	x	10,000	=	_,_ _ 0,0 0 0
4+	_____	x	30,000	=	_,_ _ 0,0 0 0
5-	_____	x	70,000	=	_,_ _ 0,0 0 0
5	_____	x	100,000	=	_ _,_ 0 0,0 0 0
5+	_____	x	300,000	=	_ _,_ 0 0,0 0 0
6-	_____	x	700,000	=	_ _,_ 0 0,0 0 0
6	_____	x	1,000,000	=	_ _ _,0 0 0,0 0 0
6+	_____	x	3,000,000	=	_ _ _,0 0 0,0 0 0
7-	_____	x	7,000,000	=	_ _ _,0 0 0,0 0 0
7	_____	x	10,000,000	=	_,_ _ _,0 0 0,0 0 0
7+	_____	x	30,000,000	=	_,_ _ _,0 0 0,0 0 0
8-	_____	x	70,000,000	=	_,_ _ _,0 0 0,0 0 0
8	_____	x	100,000,000	=	_ _,_ _ _,0 0 0,0 0 0
8+	_____	x	300,000,000	=	_ _,_ _ _,0 0 0,0 0 0
			Total Dollar Value	$	_____

Instructions:

1. For each Exposure Value, count the number of times the value appears in the row or column being considered on the Asset Exposure Form. Enter this number in the Number of Ratings column.
2. For each row multiply the number of ratings by its multiplier to obtain the Intermediate Value.
3. Add all of the intermediate values to obtain the Total Dollar Value.

Countermeasures shield or correct vulnerabilities. The portion of the ALE attributable to each vulnerability is determined in the asset exposure analysis. This information is used in the selection and application of countermeasures to test the countermeasures most likely to be cost-effective. A procedure for selecting candidate countermeasures and testing them for cost effectiveness is presented in paragraph 1.4.7. A similar procedure for selecting and testing non-cost-effective countermeasures for potential inclusion is also given.

Countermeasures being examined should be tested in combination as well as singly to determine if using more than one countermeasure has any advantage. This must be done. Often countermeasures will partially duplicate each other and a second countermeasure may provide little or no benefit. The procedure in paragraph 1.4.7 allows this test.

The effectiveness of countermeasures is rated subjectively using Table _-10. The number of attacks that successfully penetrate the countermeasure is estimated using Table _-11.

1.3.8 Worst-Case Analysis. When threats and assets are evaluated, many of the ratings are made without complete data about attack frequencies, replacement costs, etc. To take this lack of precise data into account, precision estimates are made a part of each rating.

This allows for a worst-case analysis of ALEs and levels of risk. A worst-case analysis measures how high the ALEs or levels of risk could be if all of the threat and asset evaluations were underestimated. The amount that a rating could possibly be underrated is related to the precision estimate: the more precise the rating the smaller the error.

Table _-12 is used to estimate how high the threat and asset ratings could be. The asset exposure analysis can then be redone with the new ratings.

A worst-case analysis is useful if a large number of rough ratings have been made, or if there are particularly valuable non-dollar-valued assets that

Table _-10. Ratings for Countermeasures Application

Effectiveness of Countermeasures	Rating
Very High	VH
High	H
Medium	M
Low	L
Very Low	VL

Table _-11. Countermeasures Effectiveness

Threat-Vulnerability Ratings

Countermeasure Effectiveness:	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8	8⁺
VL	0	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8
L	0	0	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺
M	0	0	0	0	1⁻	1	1⁺	2⁻	2⁻	2⁻	2	2	2⁺	3⁻	3⁻	3	3	3⁺	4⁻	4	4⁺	5⁻	5	5
H	0	0	0	0	0	1⁻	1⁻	1	1⁺	1₊	1⁺	2⁻	2⁻	2⁻	2	2	2	2⁺	2⁺	2⁺	2⁺	3⁻	3⁻	3
VH	0	0	0	0	0	0	0	0	0	0	0	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1	1	1

Instructions: Ignore precision ratings. Locate the column containing the rating for the estimated number of successful attacks before the countermeasure is applied. Locate the row containing the rating for the effectiveness of the countermeasure. The rating for the estimated number of attacks which successfully penetrate the countermeasure is found at the intersection of the row and column.

Table _-12. Estimate of Maximum Ratings

Precision Ratings

Frequency or Value Ratings	V	F	R
1^-	1^-	1	2
1	1	1^+	2^+
1^+	1^+	2^-	2^-
2^-	2^-	2	3
2	2	2^+	3^+
2^+	2^+	3^-	4^-
3^-	3^-	3	4
3	3	3^+	4^+
3^+	3^+	4^-	5^-
4^-	4^-	4	5
4	4	4^+	5^+
4^+	4^+	5^-	6^-
5^-	5^-	5	6
5	5	5^+	6^+
5^+	5^+	6^-	7^-
6^-	6^-	6	7
6	6	6^+	7^+
6^+	6^+	7^-	8^-
7^-	7^-	7	8
7	7	7^+	8^+
7^+	7^+	8^-	8^+
8^-	8^-	8	8^+
8	8	8^+	8^+
8^+	8^+	8^+	8^+

Directions: Locate the row with the frequency or asset rating for which the maximum value is to be computed. Locate the column with the precision of this rating. The maximum rating is at the intersection of the row and column.

require protection against the worst conceivable events. The results of the worst-case analysis can be used to recommend countermeasures based on a realistic but pessimistic view of the dangers to the ADP system or facility.

1.4 RISK ASSESSMENT PROCEDURES

1.4.1 Introduction. The following paragraphs present the procedures for performing the risk assessment described in paragraph 1.3. Each section must be completed before the next section can be started.

Each paragraph will describe one procedure and will contain the instructions, blank or preprinted forms, and tables for performing the procedures. If forms completed in a previous step are required, they will be noted.

1.4.2 Threat Evaluation Procedure. Threats to the ADP system or facility are identified, and the frequencies of attacks against the ADP system or facility are estimated in this step.

a. Forms and Tables Required.

1. Preprinted and blank threat evaluation forms (Figures _-7 through _-35, and Figure _-2[D]*).
2. Tables _-1[D] and _-2[D].
3. Threat Tally Sheet (Figure _-36).

b. Procedure.

(1) For each preprinted Threat Evaluation Form:

*A "D" in brackets, i.e., [D], following a figure number indicates that the figure is a duplicate of a figure found in its proper place in this document.

(a) Use Table _-1[D] to estimate the frequency of attacks against the ADP sytem or facility based upon the threat.

(b) Use Table _-2[D] to give a rating of the precision of the frequency estimate.

(c) Justify the frequency and precision ratings in the section provided. Reference any materials used to develop the ratings.

Each preprinted threat evaluation form identifies a generic threat and provides rating guidance.

(2) Identify, describe, and rate any threat that is not described on a preprinted Threat Evaluation Form. Blank threat evaluation forms are used for this purpose. The rating is made by the procedures in Step 1, above.

(3) Transfer the frequency and precision ratings for each threat to the Threat Tally Sheet, Figure _-36.

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Post-Employment Access		

DESCRIPTION

Former employees or contractor personnel may have access to the ADP system after termination of employment or a local transfer.

EXAMPLES & EVALUATION GUIDANCE

- o Former employees and contractor personnel may not be purged from access lists
- o Access may be granted solely based on personal recognition
- o Former employees and contractor personnel may retain possession of cypher lock combinations, keys, magnetic cards, passwords, or other similar means of access

EVALUATION GUIDANCE

Estimate the probable annual number of attempts to gain access to the ADP system or facility by former employees and contractor personnel after termination of employment or a local transfer. The personnel departments of the host agency and contractors can provide the yearly turnover rate of employees. Estimate how many of those former employees will attempt to gain access to the system and how often they are likely to try. The product of these will yield the probable number of attempts at access.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-7

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Disgruntled Employee or Contractor Access	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

Disgruntled employees and contractor personnel may gain access to the ADP system or facility for malicious mischief.

EXAMPLES & EVALUATION GUIDANCE

- Browsing
- Causing an intentional denial of service
- Deleting or modifying needed files
- Sending spurious messages
- Altering input or output data
- Vandalizing the system

EVALUATION GUIDANCE

Estimate the number of incidents each year involving disgruntled employees gaining access to the ADP system for the purpose of malicious mischief. Experience from other ADP systems within the same facility could be used. This estimate should be modified to reflect changes in employee morale. Recent suspensions, firings, and forced transfers may affect this estimate.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-8

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Agent Access		

DESCRIPTION

Access to the ADP system may be gained by enemy agents.

EXAMPLES & EVALUATION GUIDANCE

An agent may:

- o Assume the identity of an individual with authorized access to the ADP system or facility
- o Steal or otherwise reproduce a key, magnetic card, or other physical identifier which in turn provides access to the ADP facility
- o Gain entrance to the ADP facility by penetrating the access control measures, such as gaining entrance during a shift change when a large number of people are entering and exiting the computer facility
- o Gain entrance through bribery of guard personnel or others who control access to the ADP facility
- o Gain entrance through a service entrance, e.g., a loading dock
- o Commit acts of sabotage by gaining access to the ADP facility or adjacent areas

EVALUATION GUIDANCE

Estimate the probable frequency of attacks by enemy agents. The frequency of attacks is related to the sensitivity of the information being processed and stored at the ADP facility. For example, a facility that processes Top Secret data can expect to have a higher frequency than a facility that processes only confidential data. The installation Security Officer should be consulted for input to this estimate. The risk assessor is cautioned that this data may itself be sensitive information.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-9

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Uncleared Personnel Access		

DESCRIPTION

Uncleared personnel, e.g., visitors, maintenance staff, or customer engineers, may be allowed unescorted access or greater access than warranted.

EXAMPLES & EVALUATION GUIDANCE

- Visitors who are part of an escorted tour may become separated from the group and enjoy unescorted access to vital elements of the ADP facility such as the tape library
- Frequent visitors to the ADP facility may be allowed to escort themselves to their destinations, thus bypassing the access control and escort procedures for visitors
- Visitors may observe classified information being processed
- Visitors may observe vulnerabilities in the ADP countermeasures for the purpose of exploiting these vulnerabilities; for example, they may observe staffing of guard stations at shift change
- Visitors may plant passive devices such as hidden microphones or active devices such as bombs
- Maintenance staff and customer engineers may not be properly escorted and supervised
- Unescorted persons may commit acts of vandalism

EVALUATION GUIDANCE

Estimate the probable frequency of attacks by uncleared personnel with legitimate access to the ADP facility. Sign-in logs can provide the number of persons admitted to the facility per year. The number of uncleared personnel who have greater access than warranted should also be considered. Using the total number of uncleared people as an upper limit, the risk assessor should estimate how many of these people may misuse their privileges or attempt to gain wider privileges.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-10

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Emanations (Unintended)	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

The presence of electronic equipment in the ADP facility may cause electromagnetic emanations to be radiated great distances from the ADP facility. These emanations may be decipherable into useful information.

EXAMPLES & EVALUATION GUIDANCE

- Personally-owned tape players, radios, or television sets located at the computer console may be a source of emanations
- Telephones may allow conversations within the computer room to be overheard remotely
- Facility equipment may violate TEMPEST standards

EVALUATION GUIDANCE

Estimate the probable frequency of attempts to obtain information by using emanations from electronic equipment within the ADP facility. The facility Security Office should be contacted for information.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-11

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Emanations (Covert)		

DESCRIPTION

An agent may place or cause electronic equipment to be placed within or adjacent to the ADP facility to transmit electromagnetic signals. These signals may be intelligible, thus compromising the information being processed.

EXAMPLES & EVALUATION GUIDANCE

- Listening devices may be planted in the ADP equipment by customer engineers who maintain the equipment
- Listening devices may be planted in the computer room by unsupervised maintenance personnel or by unescorted visitors

EVALUATION GUIDANCE

Estimate the probable frequency of attempts to place electronic equipment within the ADP facility to obtain information. The frequency of attack is related to the sensitivity of the information being processed and stored at the ADP facility. For example, a facility that processes Top Secret data can expect a higher frequency than a facility that processes only confidential data. The facility Security Officer should be consulted. Known or suspected attempts at similar installations processing similar data can be a guide. The risk assessor is cautioned that this information may itself be sensitive information.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-12

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Emanations (Interference)		

DESCRIPTION

Emanations from outside sources may interface with transmission, reception, or processing of data.

EXAMPLES & EVALUATION GUIDANCE

- Radio transmitters or radar in the vicinity of the ADP facility may interfere with computer operation
- Electronic laboratories in the vicinity of the ADP facility may unintentionally produce electromagnetic emanations that may disrupt computer functions

EVALUATION GUIDANCE

Using past experience, estimate the frequency of occurrences of disruptive emanations from outside sources. A survey of possible sources of electromagnetic emanations in the area is suggested.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-13

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
Improper Marking of Classified or Sensitive Output	RATING (TABLE _-1)	PRECISION (TABLE _-2)

DESCRIPTION

Information produced by the ADP system, e.g., computer printouts, tapes, and disks, may not be properly marked to indicate sensitivity or classification.

EXAMPLES & EVALUATION GUIDANCE

- Personnel may fail to mark properly computer-produced information or to determine its correct sensitivity or classification. For example, computer dumps containing classified or sensitive information may be downgraded without adequate review, or tapes containing classified or sensitive information may be labeled incorrectly
- Personnel may accept computer-produced labels on computer printouts without manually reviewing the information to determine the accuracy of the markings
- Improperly marked messages may be incorrectly distributed
- Diagnostic computer printouts, e.g., operating system dumps, may contain classified sensitive information but be marked inappropriately

EVALUATION GUIDANCE

Estimate the probable frequency of disclosures of data as a result of improper marking. Estimate the number of printouts, tapes, and disks. Estimate the proportion of these that is likely to be marked improperly and disclosed. The unauthorized disclosure may be to an unfriendly agent or to a co-worker.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-14

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
Improper Handling of Classified or Sensitive Information	RATING (TABLE _-1)	PRECISION (TABLE _-2)

DESCRIPTION

Information (even though it is marked appropriately) may be handled improperly.

EXAMPLES & EVALUATION GUIDANCE

- Classified or sensitive computer-produced information may be improperly protected and accounted for. For example, classified or sensitive working papers may not be destroyed or entered into the document control system within the required time period
- Passwords and other identifiers which can be used to log-on or otherwise gain access to the ADP system may not be properly protected; for example, they may be written on desk calendars
- Messages may receive wider distribution than authorized or intended
- Wrong tapes and disks may be mounted. Classified disks might remain mounted during unclassified processing activity. Classified tapes might be mounted upon request, though not authorized

EVALUATION GUIDANCE

Estimate the probable frequency of disclosures of data as a result of improper handling. Estimate the number of printouts, tapes, and disks. Use these data to estimate the number of items that may possibly be mishandled.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-15

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
Employee or Contractor Fraud	RATING (TABLE _-1)	PRECISION (TABLE _-2)

DESCRIPTION

Employees or contractor personnel having access to the ADP system may attempt to manipulate the ADP system to commit fraud. In doing so, personal data or other sensitive information may be compromised or modified.

EXAMPLES & EVALUATION GUIDANCE

- Input data may be falsified
- Unauthorized software may be used
- Output reports may be falsified
- Control and audit procedures may be subverted

EVALUATION GUIDANCE

Using your judgment and past experience, estimate the frequency of attempted or successful fraud. The type of data processed should be considered. A facility that prepares a payroll or dispenses funds is a likely candidate for fraud. Consult the facility Security Officer for information on past frauds.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☒ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-16

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Alteration of ADP System Software		

DESCRIPTION

Employee or contractor personnel may alter the ADP system software in an unauthorized manner.

EXAMPLES & EVALUATION GUIDANCE

- A computer program may be inserted into the ADP system to:
  - -- Masquerade as the log-on program and illicitly obtain user passwords
  - -- Illicitly gain access to information stored within the ADP system
  - -- Record statistics such as the number, frequency, and distribution of file accesses or resource usage for traffic analysis
- A computer program may be executed in the ADP system that penetrates the operating system (in effect taking control from the operating system) and thereby gains access to all of the information accessible to and protected by the operating system
- A computer program may gain access to the wrong data or source file and alter its contents
- An existing program may be modified to accomplish the above ends

EVALUATION GUIDANCE

Estimate how frequently software and data are altered accidently or intentionally. Programming errors, incorrect job streams, and overwrites that would alter the ADP software should be considered. The frequency of intentional modification to software by personnel to obtain unauthorized information is part of the frequency estimate. Consult system programers responsible for correcting these problems.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-17

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Alteration of ADP System Hardware	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

Employee or contractor personnel may alter the ADP hardware configuration in an unauthorized manner.

EXAMPLES & EVALUATION GUIDANCE

- o Maintenance personnel may disable security-relevant subsystems
- o A malfunctioning terminal may be replaced by a different type or model terminal by a user
- o Listening devices can be inserted during replacement of components
- o Altering hardware may cause secondary damage to equipment

EVALUATION GUIDANCE

Estimate how frequently unauthorized modifications of ADP system hardware are made. Using past experience, estimate how often an additional terminal or other piece of hardware has been connected to the system without approval. Also consider switching of physical devices. The customer engineer may be able to provide information about hardware modifications and changes made to the authorized configuration.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-18

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Unauthorized Disclosure of Information	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

Employees or contractor personnel having access to classified, personal, or other sensitive information may disclose this information to other personnel. Information may also be disclosed through a malfunction of the ADP system.

EXAMPLES & EVALUATION GUIDANCE

- o Cleared personnel may assume that possession of a clearance is tantamount to a need to know
- o Cleared personnel may accept the explanation offered by a person requesting information without verifying the explanation
- o Personnel may disclose information due to personal loyalties or a desire to share interesting information
- o Uncleared personnel may overhear discussions of classified information
- o Information may be disclosed through a malfunction of the ADP system. For example, an operating system error may cause classified information to be included in unclassified output

EVALUATION GUIDANCE

Estimate the frequency of unauthorized disclosure of information. The facility Security Officer may be able to provide data on security violations involving possible compromise of information. Computer room personnel may be also able to provide data concerning disclosure of data as a result of computer error. Ask facility personnel the question: "How often have you had the opportunity to see classified information that you did not have a need to know?" Personal and other sensitive information should be included in determining the rating.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-19

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Physical Theft		

DESCRIPTION

Enemy agents, employees, contractor personnel, or outsiders may steal hardware, supplies, or information, such as printouts, magnetic media, or proprietary software from the ADP facility.

EXAMPLES & EVALUATION GUIDANCE

- o Terminals, supplies, or other physical assets may be stolen for prof by employees, contractor personnel, or persons not associated with t ADP installation
- o Agents may steal directly, or through bribery, coercion, or subterfu
- o Employee or contractor personnel may steal magnetic media by conceal them among their personal effects
- o Employees or contractor personnel may act in concert to steal inform tion. For example, computer printouts containing sensitive informat may be placed in trash receptacles for later retrieval by a confeder

EVALUATION GUIDANCE

Estimate the frequency of theft of physical assets or data on any storage medium. Inventory records are a source of determining theft of tapes and disks. The installation Security Office and local police may ha e records showing reported thefts or items that have been reported missing. Persona knowledge of the theft of items, especially physical assets and proprietar software, is useful. Incidence of theft may be related to employee morale.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-20

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Eavesdropping		

DESCRIPTION

An agent, employee, or contractor person may eavesdrop upon a telecommunications link to obtain the information being transmitted or to try to overhear classified or sensitive information being discussed.

EXAMPLES & EVALUATION GUIDANCE

- o A wiretap may be placed upon a telecommunications line
- o Information transmitted via radio, satellite, or microwave may be intercepted and analyzed

EVALUATION GUIDANCE

Estimate the frequency of attempts at eavesdropping at the facility. The facility Security Officer may be able to provide data. Incidents of eavesdropping are related to the sensitivity and classification of data being processed.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-21

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Misuse of Computer Resources	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

Individuals may employ the resources of the ADP system for unauthorized purposes and deny the use of the ADP system for authorized purposes.

EXAMPLES & EVALUATION GUIDANCE

- Individuals may employ the resources of the computer system to:
  - -- Test various features or to execute unusual programs to see how the computer system responds
  - -- Develop and play computer-based games
  - -- Carry out unauthorized software development related to course assignments for school
  - -- Examine the various files on the system or browse for residue in main memory or on mass-storage devices
- Individuals may sell the computer resources for personal gain
- Contractor personnel in particular may use the computer resources for conducting benchmark tests or for software development unrelated to their contractual use of the ADP system

EVALUATION GUIDANCE

Estimate the frequency of unauthorized use of the ADP system by authorized users. System accounting tapes or audit trails may be useful. The availability of interesting games will affect the frequency. The inquisitiveness and creativity of personnel will also affect the frequency.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-22

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Intentional Denial of Service (Software)		

DESCRIPTION

An individual may intentionally deny the use of the computer resources to authorized users by excessive use of system resources.

EXAMPLES & EVALUATION GUIDANCE

An individual may:

- Cause multiple programs to be executed, thus saturating the ADP system
- Cause a program to request excessive amounts of mass storage, thus denying the use of this resource to other users
- Cause a program to use excessive central processor time, thus denying the use of the processor to other users
- Cause a program to request excessive operating system services to deny the use of this service to other users. For example, a program that makes repeated requests for the time of day may impair the synchronization of certain time-dependent programs that must also request the time of day

EVALUATION GUIDANCE

Estimate the frequency of attempts at intentional denial of service of users. How often was the system saturated during the past year due to the excessive CPU time or storage requirements of a single program? How often were such saturations avoided by operator action? The computer operator, shift supervisors, experienced personnel, and system logs may be able to provide data.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-23

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Intentional Denial of Service (Hardware)		

DESCRIPTION

An individual may intentionally deny the use of the computer resources to authorized users by interrupting the operation of system hardware.

EXAMPLES & EVALUATION GUIDANCE

- o Pulling power cord
- o Removing necessary hardware
- o Vandalism
- o Altering switch settings to cause incompatibility of hardware

EVALUATION GUIDANCE

Estimate the frequency of attempts to cause intentional denial of service by altering hardware. The computer operator, shift supervisor, guards, and other personnel may be able to provide data. Suspicious or unusual incidents should be considered.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-24

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Power Instability	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

A power fluctuation or interruption may occur, denying the use of the ADP system to authorized users or altering information being processed.

EXAMPLES & EVALUATION GUIDANCE

- o A power fluctuation or "spike" may cause the ADP system to become inoperable, or to destroy or change data being stored or written
- o A complete interruption of power (power line outages, blackouts, etc.) can cause a long-term denial of service unless alternative power sources are available
- o Power fluctuations can damage equipment

EVALUATION GUIDANCE

Estimate the frequency of outages and surges in primary power supply. Contact the facility or building manager and the local power company for data. Consider all causes of power outages and surge.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-25

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Telecommunications Failure	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

The telecommunications links for the ADP system may fail and deny the use of the ADP system to remote users who depend on the telecommunication links.

EXAMPLES & EVALUATION GUIDANCE

- o The telecommunications links may be deliberately destroyed
- o Natural events such as storms may disrupt the telecommunications links
- o Switching devices may fail

EVALUATION GUIDANCE

Estimate the frequency of telecommunications failures. Ask for data from the computer facility manager, telephone company, or other providers of communications links. Consider terrestrial, satellite, and microwave telecommunications.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-26

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Environmental Control Failure		

DESCRIPTION

The air conditioning, heating, or humidity controls may malfunction and deny the use of the ADP system to authorized users.

EXAMPLES & EVALUATION GUIDANCE

- On very hot days, the air conditioning system may fail due to overstress
- Humidity controls may malfunction, allowing the humidity to become excessive

EVALUATION GUIDANCE

Estimate the frequency of environmental control system failures. Contact the facility or building manager for data. The manufacturers of the environmental control systems can also supply data.

IMPACT

DESTRUCTION ☐ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-27

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Sabotage		

DESCRIPTION

The ADP system or facility may be destroyed either in whole or in part by acts of sabotage.

EXAMPLES & EVALUATION GUIDANCE

- o An agent may physically damage the computer hardware or storage media
- o A bomb may destroy the ADP facility
- o Political groups may take physical action against the ADP facility
- o Local residents unhappy because of an installation activity may attem to sabotage the ADP facility

EVALUATION GUIDANCE

Estimate the frequency of destruction by sabotage. Prior incidents at the computer facility or similar installations should be considered. The installation Security Officer and police may be able to provide estimates. Location and political climate are of great importance.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-28

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Weather Damage		

DESCRIPTION

The ADP system or facility may be destroyed in whole or in part by severe weather, e.g., a hurricane, thunderstorm, tornado, windstorm, or hailstorm. Severe weather may be common in some locations.

EXAMPLES & EVALUATION GUIDANCE

- The ADP facility may be damaged by leaking roofs, damaged windows, or falling objects
- Damage to shipboard computers may be caused by objects not properly secured

EVALUATION GUIDANCE

Estimate the frequency of destruction or disruption caused by the weather. The National Weather Service can provide information. Historical data should be used. The National Bureau of Standards' FIPS Pub 31 discusses the threat of weather. Ships' logs may be useful for estimates of shipboard damage.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-29

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Natural Disaster		

DESCRIPTION

The ADP system or facility may be destroyed in whole or in part by a natural disaster such as an earthquake, tidal wave, mud slide, or bursting dam. Natural disasters are rare but catastrophic events.

EXAMPLES & EVALUATION GUIDANCE

- o ADP systems and facilities are subject to damage from natural disasters. Damage resulting from these threats can be catastrophic

EVALUATION GUIDANCE

Estimate the frequency of destruction or disruption by earthquake, tidal wave, bursting dams, or other natural disasters. Contact the National Weather Service and building manager for information. Use historical data. Anticipating the frequency and severity of these occurrences is difficult to accomplish with accuracy. The potential for occurrence should be considered. The National Bureau of Standards' FIPS Pub 31 provides information on evaluating the frequency of natural disasters.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-30

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Water Damage (Internal)	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

Leakage from a supporting structure's water supply system may damage the ADP facility.

EXAMPLES & EVALUATION GUIDANCE

- Water pipes above the computer room may leak or burst causing damage to the computer equipment
- Sprinkler systems may be activated inadvertently

EVALUATION GUIDANCE

Estimate the frequency of burst pipes, accidental sprinkler activations, and other events that could release water inside the building. Contact the building manager or appropriate shipboard officers for information.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-31

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Water Damage (External)	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

Flooding from surface runoff, rivers, tides, or other external sources may damage the ADP facility.

EXAMPLES & EVALUATION GUIDANCE

- o A flood or high tide may destroy or damage the ADP installation
- o Flooding of a shipboard facility may be caused by rough seas

EVALUATION GUIDANCE

Estimate the frequency of occurrence of external conditions that could cause water damage. The building manager, ship's engineer, and National Weather Service should be contacted for information.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-32

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Fire (Internal)	(TABLE _-1)	(TABLE _-2)

DESCRIPTION

A fire may develop within the ADP facility and destroy the facility in whole or in part.

EXAMPLES & EVALUATION GUIDANCE

- o A fire may destroy the ADP facility and/or supporting facilities, e.g., tape storage
- o Electrical fires may occur inside the computer room
- o Paper supplies inside the ADP facility may catch fire

EVALUATION GUIDANCE

Estimate the frequency of fires inside the facility. Contact the ADP faci manager, building manager, ship's engineer, and fire marshal for informati Examine histories of similar facilities.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-33

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Fire (External)		

DESCRIPTION

A fire in a neighboring area may spread and destroy the ADP facility and/or supporting facilities. Adjacent areas may present significant fire hazards, different from those within the facility, to the ADP facility.

EXAMPLES & EVALUATION GUIDANCE

- o Neighboring buildings may contain highly flammable materials
- o Neighboring buildings may have hazardous work being performed in them that is highly susceptible to fire
- o Forest or brush fires may spread and destroy the ADP installation
- o A fire in another part of the building or vessel housing the ADP facility, e.g., a kitchen, may spread to the ADP facility

EVALUATION GUIDANCE

Estimate the frequency of fires outside the computer facility that are close enough to affect the facility. Actual fires and probability of fire in adjoining buildings, offices, or adjoining areas of a ship should be considered. Contact the fire marshal, ship's engineer, and neighboring building managers for information.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-34

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)
Enemy Overrun		

DESCRIPTION

ADP facilities may be overrun by enemy forces.

EXAMPLES & EVALUATION GUIDANCE

- o A fixed installation may be attacked and captured by enemy forces
- o Shipboard ADP systems will be affected by the seizure of the ship they are on
- o Facilities and systems on U.S. Navy vessels may be damaged in a military operation
- o An attack that does not overrun the ADP facility may damage it or damage its support facilities

EVALUATION GUIDANCE

Estimate how frequently the ADP system or facility is likely to be overrun or seized by hostile forces. This will depend a great deal upon the mission and location of the ADP system or facility. For mobile systems, the frequency may vary with the location. This estimate may be sensitive information. Consult the installation's Security Officer and Naval Intelligence for guidance

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☐ DENIAL OF SERVICE ☒

JUSTIFICATION

Figure _-35

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING (TABLE _-1)	PRECISION (TABLE _-2)

DESCRIPTION

EXAMPLES & EVALUATION GUIDANCE

IMPACT

DESTRUCTION ☐ DISCLOSURE ☐ MODIFICATION ☐ DENIAL OF SERVICE ☐

JUSTIFICATION

Figure _-2 [D]

Table _-1[D]. Frequency of Attacks

Frequency	Rating
Never	0
Once in 300 years	1
Once in 30 years	2
Once in 3 years	3
Once every 4 months or 3 times a year	4
Once a week or 52 times a year	5
Once a day or 365 times a year	6
Once every 2 hours	7
Once every 15 minutes	8

Note: Ratings may be modified by $^{+}$ for "more often than" or $^{-}$ for "less often than". For example, 3^{+} is more often than every 3 years and 3^{-} is less often than every 3 years.

Table _-2[D]. Precision of Estimate

Precision	Rating
Very Precise	V
Fairly Precise	F
Rough	R

THREAT TALLY SHEET

THREAT	FREQUENCY RATING	PRECISION
Post-Employment Access		
Disgruntled Employee Access		
Agent Access		
Uncleared Personnel Access		
Emanations (Unintended)		
Emanations (Covert)		
Emanations (Interference)		
Improper Marking		
Improper Handling		
Fraud		
Alteration of Software		
Alteration of Hardware		
Disclosure of Information		
Physical Theft		
Eavesdropping		
Misuse of Resources		
Intentional Denial (Software)		
Intentional Denial (Hardware)		
Power Instability		
Telecommunications Failure		
Environmental Control Failure		
Sabotage		
Weather Damage		

Figure _-36 (Page 1 of 2)

THREAT TALLY SHEET (Continued)

THREAT	FREQUENCY RATING	PRECISION
Natural Disaster		
Water Damage (Internal)		
Water Damage (External)		
Fire (Internal)		
Fire (External)		
Enemy Overrun		

Figure _-36. (Page 2 of 2)

1.4.3 Vulnerability Evaluation Procedure. The vulnerabilities of the ADP system or facility are identified and their severity estimated in this step.

a. Forms and Tables Required.

1. Preprinted and blank vulnerability evaluation forms (Figures _-37 through _-61 and Figure _-4[D]).

2. Table _-3[D].

3. Vulnerability Tally Sheet (Figure _-62).

b. Procedure.

(1) For each preprinted Vulnerability Evaluation Form:

(a) Use Table _-3[D] to rate the level with which the ADP system or facility possesses the particular vulnerability.

(b) Justify the rating in the space provided. Each preprinted Vulnerability Evaluation Form describes a generic vulnerability of ADP systems and facilities and provides guidance for rating the vulnerability.

(2) Identify, describe, and rate any system or facility vulnerability which is not described on a preprinted Vulnerability Evaluation Form. Blank vulnerability forms are used for this purpose. The rating is made by the procedure described in Step 1, above.

(3) Transfer the level rating for each vulnerability to the Vulnerability Tally Sheet, Figure _-62.

Vulnerability Evaluation Form

VULNERABILITY NAME	VULNERABILITY LEVEL
Covert Operating System Modifications	(TABLE _-3)

DESCRIPTION

The computer operating system may contain intentional modifications that render the operating system vulnerable to attack.

EXAMPLES & EVALUATION GUIDANCE

- Trap door. Operating systems may contain an intentionally placed function called a "trap door." The purpose of a trap-door function is to bypass the security of the operating system. Typically, a trap-door function is activated by a specific code or parameter sequence.

- Trojan Horse. Operating systems may contain a function or subroutine that performs some operation instead of, or in addition to, the service it is supposed to provide, thus bypassing the security measures.

EVALUATION GUIDANCE

The rating should be based upon the origin of the system.

If a standard release of a general-purpose operating system is used, the rating should be very low or low.

If a standard release has been modified or a special purpose operating system is used, the vulnerability can be higher depending on the benefit to be gained by the individuals with the ability to insert the flaws. Good review procedures during the software development will reduce this vulnerability. In these cases the vulnerability will range from very low to medium, with low being the most likely.

Consult an operating system programer.

JUSTIFICATION

Figure _-37

Vulnerability Evaluation Form

VULNERABILITY NAME	VULNERABILITY LEVEL
Operating System Flaws	(TABLE _-3)

DESCRIPTION

he computer operating system may contain accidental design or implementation flaws that make it susceptible to attack.

EXAMPLES & EVALUATION GUIDANCE

- Incomplete Parameter Checking. Most general-purpose operating systems provide services based upon requests, e.g., subroutine calls, superior calls, master mode entries, by application programs. As part of the request, parameters are often provided specifying the type of service, location of work areas, and other information relevant to the request being made. The operating system should validate completely these parameters before acting on the request for service. However, many operating systems do not completely check these parameters, or they make assumptions about the parameters that may not be true. For example, the operating system may assume that an address pointing to a return buffer is within the address space allocated to the requesting program. The return address might point to an area within the operating system itself. Thus in carrying out such a request the operating system would overwrite a portion of its own memory space.

- Asynchronous Attack. Some general-purpose operating systems store parameters submitted as part of a request for service in memory space accessible to applications programs. One scenario based upon an asynchronous attack is the following: An application program makes a request for service and submits a valid set of parameters. The operating system edits and accepts these parameters. However, the application program causes these parameters to be overwritten using asynchronous input/output after they have been edited by the operating system but before the request for service is carried out. When the operating system actually executes the request for service, the parameters have been altered. Various outcomes are possible, e.g., a penetration of the operating system or an intentional denial of service.

JUSTIFICATION

Figure _-38. (Page 1 of 3)

Operating System Flaws (Continued)

- o Browsing. Operating systems may have flaws that make information (called "residue" in this context) available in various buffers, temporary storage areas, or other places that may be accessible to application programs. For example, a program may request a storage buffer for the purpose of browsing for residue left there by other programs.

- o Misrouting. Operating systems may contain flaws that cause information to be misrouted (for example, written to the wrong terminal). In some cases the misrouting could be triggered intentionally by causing a specific condition to occur that in turn causes a misrouting. Seldom-used operating system functions may contain such flaws. These flaws may not be discovered due to their infrequency of use but may be intentionally exploited to cause a misrouting.

- o Deadlocks. Operating systems may contain flaws which can be exploited by application programs to cause the operating system to enter a deadlock situation. This is an unplanned-for situation in which the operating system cannot continue. Typically the operating system must be restarted in order to resume processing. An example of deadlock is a case in which two functions within the operating system are in a wait-state, with each function waiting for the other to be completed.

- o Masquerading. Operating systems may contain flaws that permit unauthorized programs to masquerade as part of the operating system. For example, an applications program may be able to masquerade as the log-on routine and obtain the user's log-on parameters. It may also be possible to have user-selected routines substituted in place of operating system routines. A user routine may be substituted for the file system routine in order to bypass the normal protection mechanisms.

- o Imbedded Passwords. The operating system may have imbedded and well-known passwords as part of the standard operating system release. Unless these passwords are changed, it may be relatively easy to invoke the operating system functions protected by these passwords.

- o Undocumented Functions. Operating systems may contain undocumented or little-known functions. These are often intended for use in operating system diagnosis, operating system maintenance, or debugging in special instances. The use of these functions may provide a means to subvert the security of the operating system. Since these functions are thought to be little known, they may be poorly protected (not password protected for example) and allowed special privileges.

- o Denial of Service. Operating systems may not be able to prevent an unauthorized denial of service. A computer program may be able to use excessive amounts of computer resources such as central processor time, temporary peripheral storage, or operating system services so that other computer programs are effectively prevented from obtaining service.

Figure _-38. (Page 2 of 3)

Operating System Flaws (Continued)

EVALUATION GUIDANCE

The rating should be made based upon a knowledge of the past performance of the operating system and its origin.

The number of flaws known to exist will provide a starting point. Also consider the number of flaws which have been found in the past and have been corrected, since they will give an indication of how many undiscovered flaws may exist.

Standard releases of general-purpose operating systems will rate no lower than medium. Specialized operating systems will rate no lower than medium unless special security features are used, such as a security kernel or extensive accreditation procedures.

Consult an operating system programer.

Figure _-38. (Page 3 of 3)

Vulnerability Evaluation Form

VULNERABILITY NAME Application Software	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The application software may contain design or implementation flaws that could lead to a compromise of security.

EXAMPLES & EVALUATION GUIDANCE

- o Improper Marking. The application software may not properly mark classified or sensitive computer-produced information.

- o Imbedded Information. The application software may contain imbedded passwords or other sensitive information. This information could be disclosed inadvertently or perhaps not marked properly.

- o Error Handling. Application software which is designed to handle errors can often cause unwanted disclosures and possible denials of service.

EVALUATION GUIDANCE

The rating should consider the likelihood that application programs contain faults that could either disclose or destroy information or cause denial of service. Only programs that have legitimate access to classified data need be evaluated for flaws that could lead to disclosure. Application programs can cause denial of service in a number of ways; for example:

- o Excessive service requests
- o Failure to perform
- o Infinite looping
- o Crashing the system

Vulnerability will be greater if persons in a position to benefit from flaws have the opportunity to insert them. The rating should be based on how common the flaws are likely to be and how damaging the consequences of these flaws could be. Historical information can be used.

Unless certification of applications software has been done, the rating will be no lower than medium.

Consult the individual applications managers.

JUSTIFICATION

Figure _-39.

Vulnerability Evaluation Form

VULNERABILITY NAME Communication Software	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The communication software may be vulnerable due to design or implementation flaws. These flaws could lead to a denial of service or a disclosure of information.

EXAMPLES & EVALUATION GUIDANCE

- Lost Messages. Messages may become lost in a communications system. Depending upon the particular system, these messages may be acknowledged as delivered. Lost messages may occur at random intervals for unknown reasons. It may be possible to cause the communications system to lose messages by saturating the system with dummy messages.

- Misrouting. Messages may be delivered to the wrong destination. As with lost messages, this condition may occur at random or be caused by exploiting a design or implementation flaw.

- Stragglers. Duplicates of messages may be created and ultimately delivered. Messages may be long delayed and delivered. The recipient may misinterpret these straggler messages.

- Interleaved Messages. A message originating at a host may be interleaved with another message, or two messages may be appended. This could result in a disclosure of information, especially if the interleaved messages are of different sensitivity.

- Signaling. Information may be transmitted in the form of patterns. Information may be placed within unused fields in a message header. The timing and length of messages can also act as signaling patterns.

- Flow Control. Flow control information may be falsified to indicate communication system congestion. This can result in a denial of service.

JUSTIFICATION

Figure _-40. (Page 1 of 2)

Communication Software (Continued)

EVALUATION GUIDANCE

The rating should be based on past performance of the software, origin of the software, and certification procedures.

The communications software of standard military networks and network front ends will rate very low or low.

Consult a communications software programer.

Figure _-40. (Page 2 of 2)

Vulnerability Evaluation Form

VULNERABILITY NAME	VULNERABILITY LEVEL
Inadequate Audit and Security Mechanisms	(TABLE _-3)

DESCRIPTION

Software systems that lack adequate prevention and detection mechanisms are more than normally susceptible to a disclosure of information.

EXAMPLES & EVALUATION GUIDANCE

- o Auditing. Auditing is a detection mechanism. Software may not have adequate audit safeguards to prevent fraud or misuse. For example, an inventory control program may allow updates to be made to inventory levels without editing the updates or generating a record of the event.

- o Threat Monitoring. Threat monitoring is a prevention mechanism that attempts to detect any unusual activity and to respond immediately in an appropriate manner, such as by terminating a job.

- o Sensitive Residue. Clear memory utility is a prevention mechanism that clears a section of the core when sensitive information has previously occupied that section.

- o Handshaking. Handshaking is a prevention mechanism in which two users or processes exchange identifiers to authenticate each other. These can be passwords or a sequence of challenges and responses.

EVALUATION GUIDANCE

The rating should be based upon:

- o The presence of the features listed above

- o Known loopholes in the features. For example, if password lists can be obtained by a person already on the system, the log-in procedure is of little value

- o General effectiveness of the measures. For example, one-time passwords are more effective than passwords that are used repeatedly

JUSTIFICATION

Figure _-41. (Page 1 of 2)

Inadequate Audit and Security Mechanisms
(Continued)

The following are general guidelines: A system with no protection features will rate very high. A system with only standard password protection will rate high or medium. Any system not designed with security specifically in mind rate medium or higher.

Consult operating system programers.

Figure _-41. (Page 2 of 2)

Vulnerability Evaluation Form

VULNERABILITY NAME Inadequate Error Detection	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The computer hardware may be vulnerable due to inadequate error detection, prevention, and correction features.

EXAMPLES & EVALUATION GUIDANCE

- Memory Errors. The computer hardware may be inadequate to detect single bit errors in main memory. This could lead to an undetected modification of the computer software.

- Peripheral Errors. The computer peripherals may have inadequate error detection and correction features. For example, the tape drives may have limited ability to detect and correct single bit errors.

EVALUATION GUIDANCE

The rating should be based on the following guideline:

- No error checking should result in a vulnerability of very high

- Single-bit-error checking should reduce vulnerability to medium

- Multiple-bit-error checking should reduce vulnerability to low or very low

Consult the customer engineer.

JUSTIFICATION

Figure _-42

Vulnerability Evaluation Form

VULNERABILITY NAME Inadequate Protection Features	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The computer design may lack adequate features for restricting user program privileges.

EXAMPLES & EVALUATION GUIDANCE

- Memory Access. The computer hardware may not have a means to restrict programs from obtaining access to all of the memory. Programs with unrestricted access may make improper modifications or disclosures.

- Instruction Set. The computer hardware may not have a means to prevent programs from executing all of the computer's instruction set. Programs may use unauthorized instructions to cause disclosures or modifications.

EVALUATION GUIDANCE

The rating should be based on the following guideline:

- If instruction set protection is not available, vulnerability should be very high

- If memory access controls are not present, vulnerability should be very high or high

- If memory access controls are enforced by bounds registers, the vulnerability should be medium

- If memory access controls are implemented by separate memory units or Read Only Memories, vulnerability can be low or very low

JUSTIFICATION

Figure _-43.

Vulnerability Evaluation Form

VULNERABILITY NAME Power Supply	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The power supply for the ADP facility may be inadequate to meet the facility's performance requirements.

EXAMPLES & EVALUATION GUIDANCE

- o Natural Events. The power supply system may be vulnerable to interruption due to natural events, e.g., lightning storms.

- o Sabotage. The power supply may be vulnerable to sabotage; for example, the power supply lines could be cut or the generator destroyed.

- o Level of Service. The power supply system may be vulnerable because of the level of service provided. For example, the ADP system may have no secondary power supply and the commercial power supply may suffer from frequent outages.

EVALUATION GUIDANCE

The rating should be made according to the following guideline:

VERY LOW - Reliable, multi-feeder primary power, or uninterruptible power supply, or reliable power source within the facility with backup power generator of sufficient capacity to continue operations indefinitely

LOW - Reliable primary power with backup batteries capable of supporting operations for up to two hours

MEDIUM - Reliable primary power with battery backup power capable of supporting operations for up to 45 minutes

HIGH - Generally reliable primary power; no backup power source; flywheel to smooth out spikes and provide for 15 seconds of acceptable power

VERY HIGH - Unreliable primary power source; no backup power source

Consult the local power company and the installation's Facility Engineer for rating guidance.

JUSTIFICATION

Figure _-44.

Vulnerability Evaluation Form

VULNERABILITY NAME Environmental Support Systems	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

The environmental support systems (air conditioning, heating, and humidity controls) may be inadequate to meet the system's performance requirements.

EXAMPLES & EVALUATION GUIDANCE

- Natural Events. The environmental support systems may not survive adverse natural events; for example, a storm may disable the air conditioning system.
- Design. The environmental support systems may contain basic design weaknesses or inadequacies; for example, the air conditioning system may be of insufficient capacity to maintain the proper temperature on very hot days.
- Level of Service. The environmental support systems may be vulnerable because of the level of service provided; for example, maintenance support for the heating system may not be available locally.

EVALUATION GUIDANCE

The rating should reflect the answers to these questions:

- If the environmental support system fails, how long can the system function?
- Are repairs readily available? Does a failure automatically cause a facility shutdown?
- If the environmental support system goes down because of failure or power outage, can it be restarted quickly? (Some systems have a start-up time.)
- How reliable is the environmental support system?
- Are backups available?

The rating should not be very low unless a backup system is available.

Consult the installation's Facility Engineer.

JUSTIFICATION

Figure _-45

Vulnerability Evaluation Form

VULNERABILITY NAME Building Construction	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

The construction of the building for the ADP system may be vulnerable.

EXAMPLES & EVALUATION GUIDANCE

The following are factors to consider:

- o Construction materials
- o Age of the building or other enclosure
- o Purpose; that is, whether designed for use as an ADP facility
- o Known inadequacies, such as electrical system design and capacity
- o Overhanging exposed water pipes and electrical connections
- o Location of ADP facility in relation to high-risk operations such as chemical laboratory, building heating plant, or kitchen

EVALUATION GUIDANCE

The rating should reflect judicious answers to the following questions:

- o How resistant is the enclosure to damage from weather, earthquake, fire, sabotage, etc.?
- o Is the enclosure made of combustible material that could provide fuel for a fire?
- o Is water damage due to floods, water pipes, drainpipes, or seepage likely to be a problem, and can it be localized if it occurs?
- o How easily do electromagnetic emanations penetrate the enclosure?

All of these questions are related to the type of materials used in the enclosure and the architecture of the building or other enclosure. Consult the installation's Facility Engineer and Security Officer for rating guidance.

JUSTIFICATION

Figure _-46

Vulnerability Evaluation Form

VULNERABILITY NAME Internal Physical Access Control	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

The internal design of the ADP facility may make it difficult to control the movement of persons within the ADP facility.

EXAMPLES & EVALUATION GUIDANCE

- The physical floor plan of the ADP facility may reduce security; for example, the job submission area may be in the computer room
- Internal doors may not be lockable
- There may be room dividers rather than walls

EVALUATION GUIDANCE

- If persons inside the facility have access to all facilities, the rating should be very high
- Room dividers can lower the vulnerability to high
- Solid walls and lockable doors with separation of functional areas can reduce the vulnerability to medium
- Guards and closed-circuit monitors can reduce vulnerability to very low

JUSTIFICATION

Figure _-47

Vulnerability Evaluation Form

VULNERABILITY NAME External Physical Access Control	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

The location, construction, and protection of the ADP facility may make it difficult to control outside access to the faciltiy.

EXAMPLES & EVALUATION GUIDANCE

The following are some factors to consider:

- o Location within a secure installation
- o Ability to control and monitor access
- o Number and characteristics of all exits, entrances, windows, and ventilation ducts; for example, whether doors have hinge pins mounted on the outside
- o Surveillance devices such as closed-circuit television, alarm systems, and exterior lighting
- o Location and design of guard stations

EVALUATION GUIDANCE

All possible entrances to the ADP facility must be considered. These include door, windows, loading docks, and accessible ventilator shafts.

A suggested method of rating this vulnerability is to answer the following questions:

1. Are all of the entrances either locked, guarded, or at least observable during all hours?

   (If there are entrances which are observable but not locked and/or guarded, stop here.)

2a. For entrances that rely on locks for protection, are the locks--doors and windows--and hinge pins secure?

2b. For entrances that rely on guards, does the guard have the ability to screen all persons entering?

JUSTIFICATION

Figure _-48 (Page 1 of 2)

External Physical Access Control (Continued)

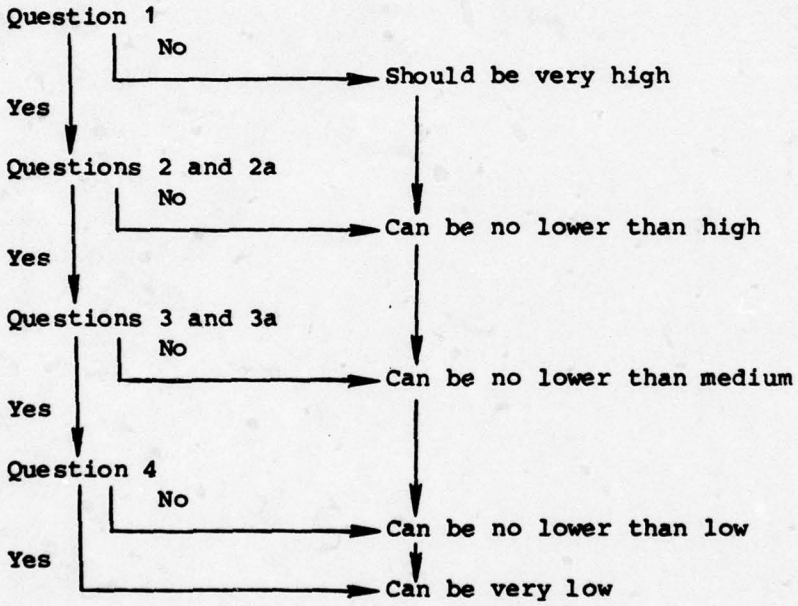
3a. For entrances that depend on locks for security, would the noise made by forcing any of these be guaranteed to alert a guard? Are there alarms on these entrances?

3b. For entrances that depend on guards for security, are the guards solely responsible for controlling access?

4. Are mantraps and remote monitoring devices used to augment the guard force?

The ratings should not be very low unless all of the above questions are answered affirmatively.

To determine the vulnerability rating, use the following rule.



Ratings may be higher than indicated if special weaknesses are noted.

Consult building diagrams and the installation's Security Office for guidance in making ratings.

Figure _-48 (Page 2 of 2)

Vulnerability Evaluation Form

VULNERABILITY NAME Inadequate Fire Protection	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

The fire protection measures may be inadequate, making the ADP facility vulnerable to fire.

EXAMPLES & EVALUATION GUIDANCE

The following are factors to consider:

- Number, type, and location of fire extinguishers
- Number, type, and location of heat and smoke detectors
- Fire wall design and locations
- Sprinkler and other fire protection systems
- Number and location of fire exits
- Routing of electrical and power cables, e.g., near heating pipes

EVALUATION GUIDANCE

The rating should reflect answers to these questions:

- Are there conditions which could cause a fire?
- Are there areas where a fire would not be noticed until it became large?
- How quickly can a fire be detected?
- How fast will a fire spread?
- How are combustible materials stored?
- Is adequate firefighting equipment available on site?
- Are personnel familiar with emergency fire procedures?
- How long will it take firefighters to respond?

JUSTIFICATION

Figure _-49. (Page 1 of 2)

Inadequate Fire Protection (Continued)

- o Can firefighters gain easy access to the ADP site?
- o Are there adequate emergency exits?

These questions should be answered about both operating and nonoperating hours. Consult the installation's Fire Marshal for rating guidance.

Figure _-49. (Page 2 of 2)

Vulnerability Evaluation Form

VULNERABILITY NAME Operations Procedures	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

The procedures for operations may not be clear or complete enough to prevent errors and to provide adequate service.

EXAMPLES & EVALUATION GUIDANCE

- o System Procedures. System start-up, shutdown, and crashes can modify data if not handled properly.
- o Production Procedures. If procedures for running programs are not complete, inappropriate data bases could be present and might be disclosed or modified.
- o User/Programer Interface. Inadequate user/programer interface procedures might result in the provision of unauthorized access or unsatisfactory service.

EVALUATION GUIDANCE

The completeness of these procedures and how well they are followed is the determining factor in these ratings. If any area is neglected, the rating will not be better than medium.

JUSTIFICATION

Figure _-50

Vulnerability Evaluation Form

VULNERABILITY NAME Software Development Procedures	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The software development procedures may not be adequate to insure that computer software is developed and controlled according to standards.

EXAMPLES & EVALUATION GUIDANCE

- Least Privilege. The software development procedures may not insure that software is developed to use the least privilege to accomplish the intended mission. For example a payroll program should not have access to all of the information in the personnel file.

- Trojan Horse. The software development procedures may not prevent unauthorized software from being inserted into the computer software under development.

- Benign Environment. The software development procedures may not produce robust and fault-tolerant software. The software environment may be assumed to be benign, that is, users will not make rare or illogical errors and the software will not be manipulated to commit fraud or to compromise security.

EVALUATION GUIDANCE

- Lack of software development procedures should result in a rating of very high

- Procedures can reduce vulnerability to low, medium, or high depending on their rigor

JUSTIFICATION

Figure _-51

Vulnerability Evaluation Form

VULNERABILITY NAME Software Acceptance Procedures	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

Procedures for the acceptance of new software may not be stringent enough to detect features that could compromise security.

EXAMPLES & EVALUATION GUIDANCE

- Quality Assurance. Quality assurance procedures for new software can prevent many problems from ever occurring, e.g., excessive core requirements, Trojan Horses, or trap doors.

- Testing and Debugging. Procedures for testing and debugging can uncover many errors in software that could be costly if the software was put into production, such as infinite loops, unrecoverable errors, or data base destruction.

EVALUATION GUIDANCE

- Lack of software acceptance procedures should result in a rating of very high or high

- Various procedures can reduce the vulnerability to high, medium, or low

JUSTIFICATION

Figure _-52

Vulnerability Evaluation Form

VULNERABILITY NAME Software Maintenance Procedures	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The procedures governing the maintenance of production computer software may have weaknesses that can lead to a compromise of security.

EXAMPLES & EVALUATION GUIDANCE

- Unauthorized Update. The software maintenance procedures may not be adequate to detect and prevent unauthorized updates from being made. Unauthorized updates could compromise the integrity of the computer software; for example, untested update changes may be applied to a check issuing program. Intentional unauthorized updates could be used to conceal an ongoing fraud, e.g., by preventing the payroll department from learning of ghost employees receiving checks.

- Incorrect Software Version. The software maintenance procedures may not be adequate to prevent incorrect or out-of-date software versions from being used. An obsolete version of the operating system might be mistakenly substituted for the current version, compromising the integrity of the production files.

- Unauthorized Access to Software. The software maintenance procedures may not be adequate to prevent unauthorized access (re-coding and copying) to the production software. Copying of the software could lead to a direct disclosure of sensitive information contained within the software. Unauthorized reading of the software might be attempted in order to detect additional vulnerabilities to exploit. The operation of a financial program might be analyzed to design a fraud.

EVALUATION GUIDANCE

- Lack of procedures should result in a rating of very high

- With procedures, the level can range from very low to high

JUSTIFICATION

Figure _-53

Vulnerability Evaluation Form

VULNERABILITY NAME Input/Output Procedures	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

An installation may have inadequate procedures for the acceptance and release of information.

EXAMPLES & EVALUATION GUIDANCE

- o Integrity Control. Without integrity procedures, information that is inaccurate, unneeded, or false may be placed in the data base--possibly causing a denial of service or fraud.
- o Service Denials. Service requests from users may not be handled because of unclear or undefined procedures for incoming transactions.
- o Information Misrouting. Inadequate input/output procedures may allow information to be delivered to an incorrect user or location.

EVALUATION GUIDANCE

- o Lack of input/output procedures, i.e., those enabling persons able to run their own jobs, should result in a rating of very high
- o Forcing submission of jobs through a clerk can reduce vulnerability to high or medium
- o Extensive identification checks and output classification monitoring by clerks can reduce the rating to low or very low

JUSTIFICATION

Figure _-54

Vulnerability Evaluation Form

VULNERABILITY NAME Supply and Service Procedures	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

Inadequate procedures for accomplishing supply and service functions can lead to unauthorized disclosure, theft, fraud, etc.

EXAMPLES & EVALUATION GUIDANCE

- o Fraud and theft may be difficult to detect if computer equipment and supplies are not accounted for
- o Stolen copies of special forms, e.g., checks, may be used to commit fraud
- o Equipment may be concealed with waste materials and recovered later

EVALUATION GUIDANCE

- o Lack of procedures controlling supply and service activities should result in a rating of very high
- o Informal supply and service can reduce the rating to high
- o Formal procedures can reduce the rating to medium
- o Formal procedures that are carefully monitored can reduce vulnerability to low or very low

JUSTIFICATION

Figure _-55

Vulnerability Evaluation Form

VULNERABILITY NAME Emergency Procedures	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

Security procedures for emergency situations may be inadequate, absent, or unenforceable.

EXAMPLES & EVALUATION GUIDANCE

- Emergency Procedures. There may be inadequate emergency procedures for a fire, flood, power failure, bomb threat, etc.
- Contingency Plans. Contingency plans may not exist to insure continuity of service if a facility, or data base, or subsystem becomes unavailable.
- Backup and Recovery. The software maintenance procedures may not provide for adequate backup and recovery. In the event that the production computer software is lost, destroyed, or rendered unusable, adequate and current backup may not be maintained. The recovery procedures may not facilitate a return to normal operations without undue risk and denial of service.
- Classified Documents and Equipment. The procedures for destroying classified material in the event of enemy overrun may be inadequate or not commonly known. These procedures are especially important to systems and facilities outside the continental United States.

EVALUATION GUIDANCE

- Lack of procedures should result in a rating of very high
- With procedures, the rating may range from high to very low, depending on how complete they are and how familiar the staff is with them

JUSTIFICATION

Figure _-56

Vulnerability Evaluation Form

VULNERABILITY NAME Security Procedures and Security Office	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

Security is a full-time job and each ADP system must have a System Security Officer (SSO). The SSO must have adequate authority to conduct an appropriate security program.

EXAMPLES & EVALUATION GUIDANCE

- o Program. The SSO is responsible for setting up a security program to protect the ADP system and facility assets as required by security policy.
- o Training. The SSO is responsible for conducting security training for all ADP facility personnel. The training should cover the broad spectrum of security, including routine operations and emergency procedures.
- o Exercise. The SSO should conduct routine security exercises to test the ADP facility for vulnerabilities.

EVALUATION GUIDANCE.
The rating is made on the basis of the comprehensiveness of the security training program and exercises. The ability of the SSO to identify computer-related security violations and to take corrective action must be considered. If the SSO does not have extensive experience in computer security, the rating will not be very low or low.

JUSTIFICATION

Figure _-57

Vulnerability Evaluation Form

VULNERABILITY NAME Management	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

Poor management attitude and policy can lead to lapses in security.

EXAMPLES & EVALUATION GUIDANCE

- o Policy. Management's policy must be well established and clearly understood. Accountability for all ADP activities should be obvious at all levels.

- o Attitude. Management's attitude toward security should be actively supportive. Personnel who see their management ignore security will likely do the same.

EVALUATION GUIDANCE

Consider the following questions for this rating:

- o Is management policy well established and clearly understood?

- o Is management's attitude toward security very supportive?

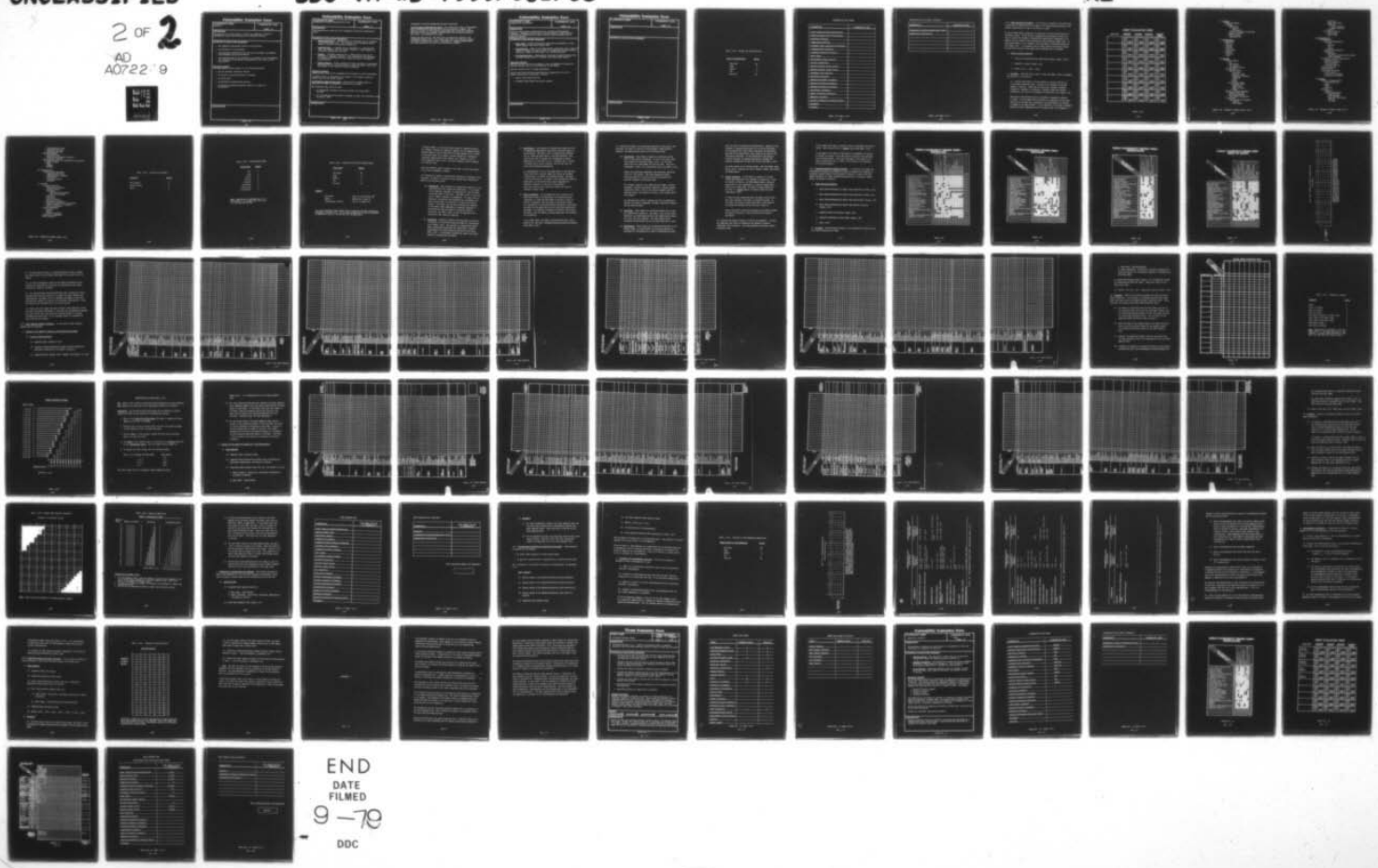
The vulnerability rating should be low or very low if both questions are answered "yes." The vulnerability rating should be medium if one question is answered "yes." The vulnerability rating should be high or very high if both questions are answered "no."

JUSTIFICATION

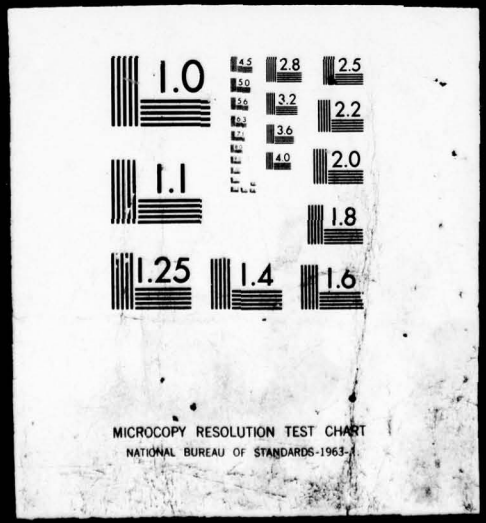
Figure _-58

AD-A072 249 SYSTEM DEVELOPMENT CORP MCLEAN VA F/G 9/2
RISK ASSESSMENT METHODOLOGY.(U)
JUL 79
UNCLASSIFIED SDC-TM-WD-7999/001/03 N000173-78-C-0455 NL

2 OF 2
AD A072 249



END
DATE FILMED
9-79
DDC



Vulnerability Evaluation Form

VULNERABILITY NAME Personnel	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

The personnel of the ADP system or facility can represent a degree of vulnerability which could be exploited to compromise security.

EXAMPLES & EVALUATION GUIDANCE

- The competency and general ability of the personnel
- The motivation of the personnel
- The personnel's satisfaction with the work environment and agreement with management policy and practices
- The trustworthiness of the personnel, as evidenced by the thoroughness and currentness of background investigations by the DISCO or some other method

EVALUATION GUIDANCE

The rating should reflect answers to the following questions:

- Are the personnel adequately trained?
- Are errors or omissions generally a problem?
- Is morale good?
- Are background investigations current?
- Are security procedures generally ignored as a matter of convenience?

JUSTIFICATION

Figure _-59

Vulnerability Evaluation Form

VULNERABILITY NAME Inadequately Protected Communications Links	VULNERABILITY LEVEL (TABLE _-3)

DESCRIPTION

The communications system may have inadequately protected communications links.

EXAMPLES & EVALUATION GUIDANCE

- Between-Lines Entry. Information may be introduced onto an otherwise idle communications link. The recipient of the information may be unable to identify this spurious information.
- Piggyback Entry. A computer may be interposed on a communications link. The computer may then inspect, discard, or alter (spoof) all information passing over the link.
- Playback. Information passing over a communications link may be recorded for subsequent playback. This vulnerability can be present on encrypted communications links unless the units of information are serialized.
- Traffic Analysis. Traffic patterns of either encrypted or unencrypted communications links may be analyzed to infer the nature, sensitivity, and content of the information being transmitted.

EVALUATION GUIDANCE

Communications lines can be wiretapped while encrypted or while unencrypted.

If several levels of vulnerability are present in the system, choose the highest level as the overall rating.

For Encrypted Communications Lines. The rating for encrypted data is based upon the type of encryption used and how it is used.

The following rules should be used:

- If DOD-approved encryption devices are used, the rating should be lower
- If a non-DoD-approved encryption technique is used, the vulnerability will be high or lower

JUSTIFICATION

Figure _-60. (Page 1 of 2)

Inadequately Protected Communications Links (Continued)

For Unencrypted Communications Lines. The vulnerability level of unencrypted data is determined by the ease with which the line may be tapped. The physical location of lines carrying unencrypted data should be considered. How easily could one be tapped? Junction boxes are the easiest places to tap a line. How accessible are they?

Outside the ADP facility, the difficulty of tapping will depend on the transmission medium used: with secure lines, very low; microwave, medium; and regular telephone line, high. Serialization, message acknowledgment, and other techniques can reduce the vulnerability somewhat.

Figure _-60. (Page 2 of 2)

Vulnerability Evaluation Form

VULNERABILITY NAME Communication Architecture	VULNERABILITY LEVEL (TABLE __-3)

DESCRIPTION

There are many possible configurations for connecting communications equipment. Depending upon the type of service required, a badly designed architectural structure could lead to various security problems such as denial of service.

EXAMPLES & EVALUATION GUIDANCE

- Heavy Loads. Properly distributed communications equipment can help reduce response time during heavy loads.
- Out-of-Service. Nodes in the communication architecture that go down can result in a denial of service unless the architecture has been properly designed to bypass the down nodes, e.g., backup facilities.
- Interruptible Lines. Communications lines may be removed from service by either natural causes or sabotage, impairing system capacity.

EVALUATION GUIDANCE

Existing military networks are medium to very low depending on backup and security features and on the survivability of the design.

Internal networks must be judged individually.

Single connections should be rated upon how vulnerable the link is to removal from service by sabotage or failure.

- Secure lines should rate low
- Telephone lines should rate high in general

JUSTIFICATION

Figure _-61

Vulnerability Evaluation Form

VULNERABILITY NAME	VULNERABILITY LEVEL (TABLE __-3)
DESCRIPTION	
EXAMPLES & EVALUATION GUIDANCE	
JUSTIFICATION	

Figure _-4 [D]

Table _-3[D]. Ratings for Vulnerabilities

Level of Vulnerability	Rating
Very High	VH
High	H
Medium	M
Low	L
Very Low	VL

VULNERABILITY TALLY SHEET

VULNERABILITY	VULNERABILITY LEVEL
Covert Operating System Modifications	
Operating System Flaws (Unintentional)	
Application Software	
Communication Software	
Inadequate Audit and Security Mechanisms	
Inadequate Error Detection	
Inadequate Protection Features	
Power Supply	
Environmental Support Systems	
Building Construction	
Internal Physical Access Control	
External Physical Access Control	
Inadequate Fire Protection	
Operations Procedures	
Software Development Procedures	
Software Acceptance Procedures	
Software Maintenance Procedures	
Input/Output Procedures	
Supply and Service Procedures	
Emergency Procedures	
Security Procedures and Security Office	
Management	
Personnel	

Figure _-62 (Page 1 of 2)

Vulnerability Tally Sheet (Continued)

VULNERABILITY	VULNERABILITY LEVEL
Inadequately Protected Communication Links	
Communication Architecture	

Figure _-62 (Page 2 of 2)

1.4.4 Asset Evaluation Procedure. In this step, the assets of the ADP system or facility are identified and the impact of an unauthorized destruction, disclosure, modification, or denial of service is rated.

In any of these impact categories, an asset may be rated as dollar-valued or non-dollar-valued. If the primary consequence of the damage is either the cost to correct the damage or a financially quantifiable consequence of the damage, then the asset is dollar-valued for that particular impact area. If the primary impact is not financial, then the asset is non-dollar-valued for that impact area. It is possible that an asset could be both dollar-valued and non-dollar-valued in some impact area, although this is unlikely.

a. Forms and Tables Required.

1. Blank Asset Evaluation Form (make extra copies) (Figure _-5[D]).

2. Examples of Assets (Figure _-63).

3. Tables _-2[D], _-4[D], _-5[D].

b. Procedure. (Whenever Table _-4[D] is used, use Table _-2[D] to estimate the precision of the rating.)

(1) Identify each asset of the ADP system or facility and list it on the Asset Evaluation Form. An asset is any resource of the ADP system or facility. Assets may be facilities, hardware, software, information, supplies, or personnel; financial assets are treated differently. Use the list of examples of assets as an aid (Figure _-63).

There may be some question about how broadly or narrowly to define an asset. For each asset that you define, all components of the asset should be in the same area, protected in the same manner, and subject to damage by the same attacks. If one component of the asset is damaged, either all other components should be highly likely to be damaged in

ASSET EVALUATION FORM

ASSET NAME	UNAUTHORIZED DESTRUCTION	UNAUTHORIZED DISCLOSURE	UNAUTHORIZED MODIFICATION	UNAUTHORIZED DENIAL OF SERVICE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ______ VALUE

Figure _-5[D]

(1) Software
- Operating System
- Programs
  - Application
    - Source
    - Non-source
  - Contract programs and packages
  - System utilities
  - Test programs
  - Communications

(2) Informational
- Operations
- Tactical
- Planning
- Defense
- Financial
- Statistical
- Payroll
- Personnel
- Other

(3) Hardware
- Central Machine
  - CPU
  - Main memory
  - I/O channels
  - Operator's console
- Storage Medium
  - Magnetic media
    - Disk pack
    - Magnetic tapes
    - Diskettes (floppies)
    - Cassettes
    - Drums
    - Other
  - Non-magnetic media
    - Punched cards
    - Paper tape
    - Paper printout
    - Other
- Special Interface Equipment
  - Network front ends
  - Data base machines
  - Intelligent controllers
- I/O Devices
  - User directed I/O devices
    - Printer
    - Card reader

Figure _-63. Examples of Assets (Page 1 of 3)

- Card punch
- Paper tape reader
- Terminals
  - Local terminals
  - Remote terminals
- Modems
- Storage I/O device
  - Disk drives
  - Tape drives

(4) Administrative
- Documentation
  - Software documentation
    - File
    - Program
    - JCL
    - System
  - Hardware documentation
  - Operations
    - Schedules
    - Operations guidelines and manuals
    - Audit documents
- Procedures (written documentation)
  - Emergency plans
  - Security procedures
  - I/O procedures
  - Integrity controls
- Inventory Records
- Other Records
- Operational Procedures
  - Vital records
  - Priority-run schedule
  - Production procedures

(5) Physical
- Resources Supply System
  - Air conditioning
  - Power
  - Water
  - Lighting
- Building
  - Structure
  - Computer operations
    - Computer room
    - Data reception
    - Tape and disk library
    - CE room
    - I/O area

Figure _-63. Examples of Assets (Page 2 of 3)

- Data preparation area
- Physical plant room
- Stationery storage

- Backup Equipment
  - Auxiliary power
  - Auxiliary environmental controls
  - Auxiliary supplies
- Waste Materials (to be considered for disclosure)
  - Magnetic media
  - Paper
  - Ribbons
  - Hardware

(6) Communications
- Communications Equipment
  - Communications lines
  - Communications processor
  - Multiplexor
  - Switching devices
  - Telephone

(7) Personnel
- Computer Personnel
  - Supervisory personnel
  - Systems analysts
  - Programers
    - Applications programers
    - Systems programers
  - Operators
  - Librarians
  - Security Officer
  - Maintenance personnel
  - Temporary employees and consultants
  - System evaluators and auditors
  - Clerical personnel
- Building Personnel
  - Janitors
  - Guards
  - Facility engineers
- Installation Management
- Other Personnel

Figure _-63. Examples of Assets (Page 3 of 3)

Table _-2[D]. Precision of Estimate

Precision	Rating
Very Precise	V
Fairly Precise	F
Rough	R

Table _-4[D]. Dollar-Valued Assets

Dollar Value	Rating
$10	1
$100	2
$1,000	3
$10,000	4
$100,000	5
$1,000,000	6
$10,000,000	7
$100,000,000	8

Note: Ratings may be modified by a + or -. For example, a 3+ is more than $1,000 and a 4- is less than $10,000.

Table _-5[D]. Ratings for Non-Dollar-Valued Assets

Value Level	Rating
Very High	VH
High	H
Medium	M
Low	L
Very Low	VL

Example:

Top Secret	High (H) to Very High (VH)
Secret	Medium (M) to High (H)
Confidential, Privacy	Low (L) to Medium (M)

All other non-dollar-valued assets such as sensitive business information, proprietary software, etc., can be rated subjectively by the risk assessor at Medium (M), Low (L), or Very Low (VL) as applicable.

a similar manner, or the entire asset should be rendered unusable. For example, consider six identical computers as six separate assets because damage to one of them would not imply damage to all of them. On the other hand, do not treat a single computer as a collection of smaller assets such as CPU, memory, etc., because if one of these components were to fail, the entire computer would be damaged to a similar level.

List the different types of assets in the order in which they appear on the list of examples of assets.

(2) Evaluate the impact of unauthorized destruction, disclosure, modification, and denial of service on each software and informational asset by the following rules:

(a) Destruction. Each software or informational asset has a cost associated with its unauthorized destruction. If the asset can be repaired, replaced, or reconstructed, then the asset is dollar-valued in this area. Use Table _-4[D] to rate the cost to repair, replace, or reconstruct. Consider costs to replace or reconstruct from documentation, management overhead, machine time, and inflation (if using the original prices). For labor, use the rate of $60,000 per man-year. If the asset cannot reasonably be repaired, replaced, or reconstructed, then the asset is non-dollar-valued in this area. Use Table _-5[D] to rate the importance of a destruction that cannot be repaired.

(b) Disclosure. Classified software and classified or sensitive information is non-dollar-valued and should be rated according to Table _-5[D]. Any software or informational assets whose unauthorized disclosure has quantifiable financial consequences are dollar-valued and should be rated using Table _-4[D]. Few software informational assets are dollar valued for unauthorized disclosure.

(c) Modification. Any software or informational asset for which an undetected modification could have a financial impact is dollar-valued. Use Table _-4[D] to estimate the financial cost of using the asset after it has been modified. This could be the cost to correct the consequences of faulty operations or a loss due to fraud. Consider cost to locate a software error, cost to recover, and the loss that can occur from fraudulent modification.

If a modification or use of the asset after it has been modified would have a serious impact that cannot be assigned a dollar-value, the asset is non-dollar-valued. Use Table _-5[D] for the rating. An asset is only non-dollar-valued for modification if the modification cannot reasonably be detected, corrected, or the use of the modified asset has a result which cannot be correct and cannot be assigned a dollar value.

(d) Denial of Service. If the temporary loss of service of an asset could lead to the destruction of non-dollar-valued information or cause the ADP system or facility to fail to fulfill its mission, then the asset is non-dollar-valued. If a destruction of non-dollar-valued information could occur, the asset has the same rating as the information potentially destroyed. If inability to perform the mission could result, use Table _-5[D] and assign a rating based upon the importance of the mission.

In all other cases, the asset is dollar-valued and a rating based on the cost due to delayed processing should be assigned using Table _-4[D].

(3) Evaluate the impact of unauthorized destruction, disclosure, modification, and denial of service of each hardware, administrative, physical, and communications asset by the following rules:

(a) Destruction. These types of assets are non-dollar-valued only if they cannot be replaced. If this is the case, their worth should be rated using Table _-5[D]. Any of these assets which are replaceable are dollar-valued. Rate their replacement, repair, or reconstruction cost using Table _-4[D].

Consult the purchasing department, GSA schedules, OMB directive A-71, and vendors. The Field Engineering Center maintains facility information and can be consulted for physical equipment and hardware costs.

For hardware, physical, and communications assets, consider management overhead, maintenance personnel, engineer support, installation costs, costs of any special hardware used on a temporary basis, and inflation, as well as the actual cost of the hardware.

For administrative assets, consider the cost to redevelop or replace from copies, management overhead, secretarial support, and any printing costs.

(b) Disclosure. These assets are non-dollar-valued only if they are classified or sensitive. Use Table _-5[D] to rate these. Generally, only some administrative and communications assets will fall into this category. All other assets can be considered dollar-valued and can be rated using Table _-4[D].

(c) Modification. These assets are non-dollar-valued only if the primary impact of a modification is incorrect operation or disclosure of information as a result of modification rather

than the cost of correcting the modification. Generally, only hardware or communications assets can be non-dollar-valued. If the modification could cause a disclosure of information, make the rating using Table _-5[D] based on the value of the information disclosed. If the modification could cause a critical operation to perform incorrectly, consider the possible consequences and make the rating using Table _-5[D].

All other assets will be dollar-valued. Rate the impact using Table _-4[D]. Consider the cost to detect, locate, and correct the modification.

(d) Denial of Service. If the denial of service of an asset causes some operations to be delayed, the asset has a value for denial of service. If these delays cause a financial penalty due to late completion or a loss of revenue due to inability to accept jobs, the asset is dollar-valued and the cost of a typical denial of service should be rated using Table _-4[D].

If there are some operations where the delay could be more than just financial, the asset is non-dollar-valued. In this case, the rating is made using Table _-5[D] based on the operations delayed and how critical a delay is.

These assets may be both dollar-valued and non-dollar-valued for denial of service if they could delay both types of operations.

(4) Evaluate the impact of denial of service of personnel. If there are operations that would be delayed by the absence of certain individuals (key personnel), rate those personnel as having a denial-of-service value.

If the delays would cause a financial loss, the personnel are dollar-valued. Rate the cost due to a typical delay using Table _-4[D].

If the impact of the delay is destruction of information or failure to perform the mission of the ADP system or facility, the personnel are non-dollar-valued. Rate them using Table _-4[D] based on the type of information lost, or Table _-5[D] based on the importance of the failed mission.

1.4.5 Threat/Vulnerability Merger Procedure. In this step, the threat and vulnerability ratings are considered in pairs to estimate the frequency of successful attacks against the ADP system or facility in each of the four impact categories of threat (unauthorized destruction, disclosure, modification, and denial of service).

a. Forms and Tables Required.

1. Blank Threat/Vulnerability Merger Form--Destruction (Figure _-64).

2. Blank Threat/Vulnerability Merger Form--Disclosure (Figure _-65).

3. Blank Threat/Vulnerability Merger Form--Modification (Figure _-66).

4. Blank Threat/Vulnerability Merger Form--Denial of Service (Figure _-67).

5. Completed Threat Tally Sheet (Figure _-36).

6. Completed Vulnerability Tally Sheet (Figure _-62).

7. Table _-6[D].

b. Procedure. The following procedure is to be performed for each of the four threat/vulnerability forms.

THREAT/VULNERABILITY MERGER FORM—DESTRUCTION

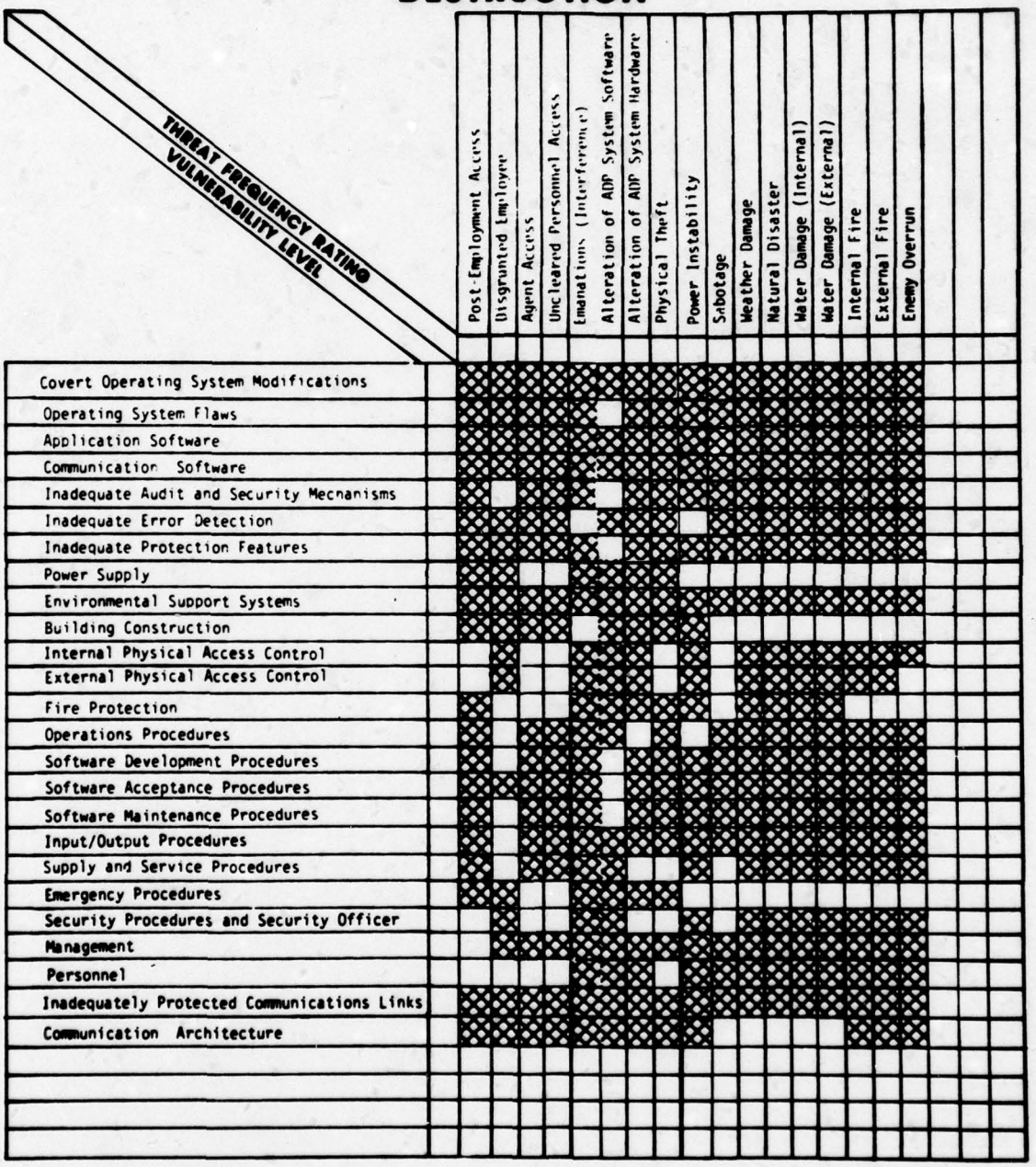


Figure _-64

THREAT/VULNERABILITY MERGER FORM—DISCLOSURE

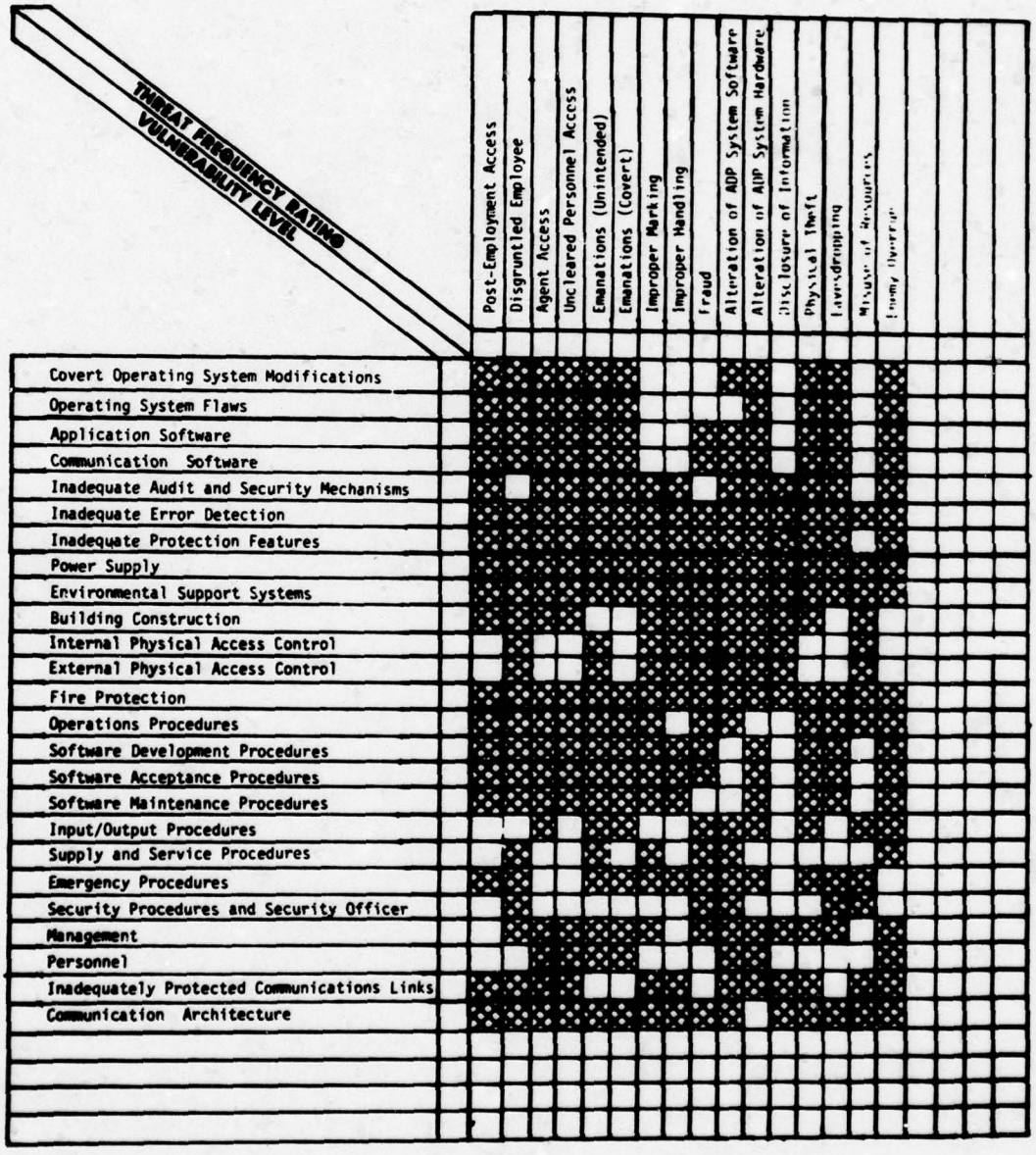


Figure _-65

THREAT/VULNERABILITY MERGER FORM—MODIFICATION

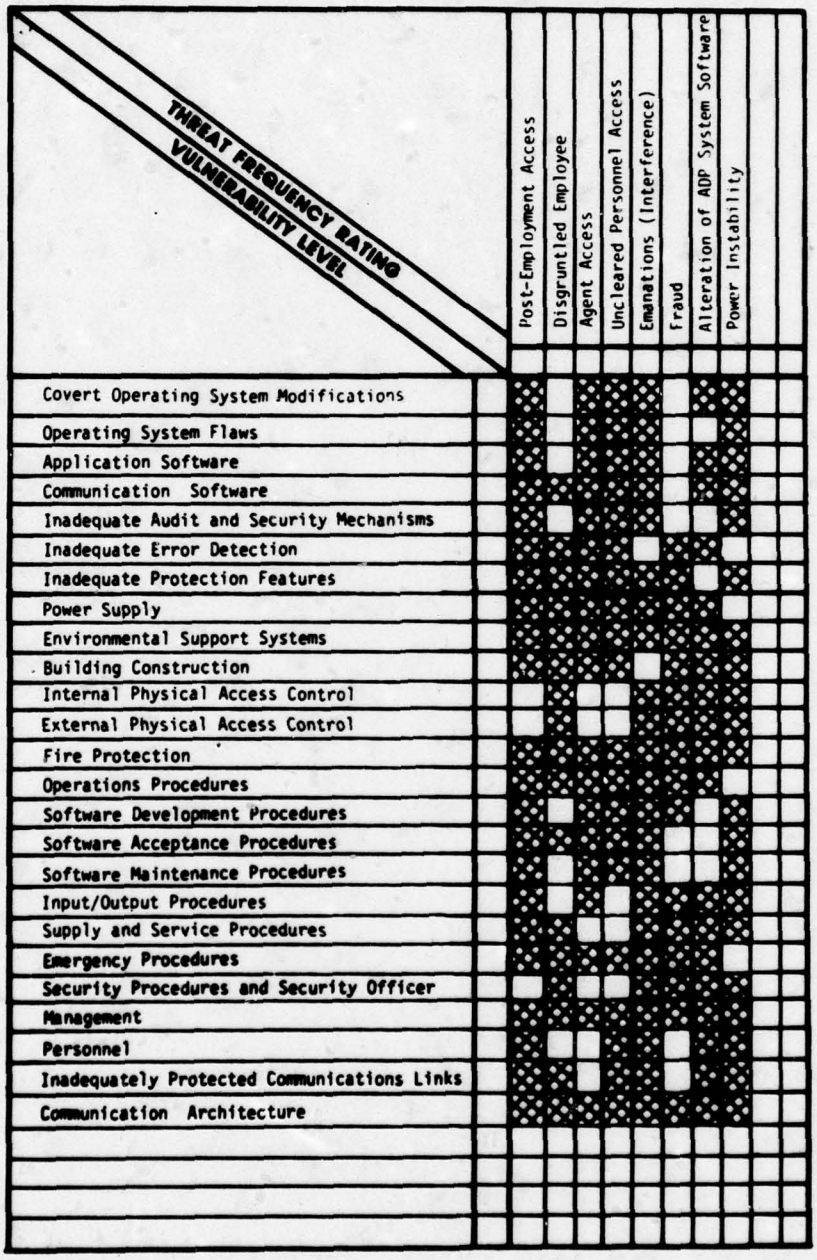


Figure _-66

THREAT VULNERABILITY MERGER FORM-
DENIAL OF SERVICE

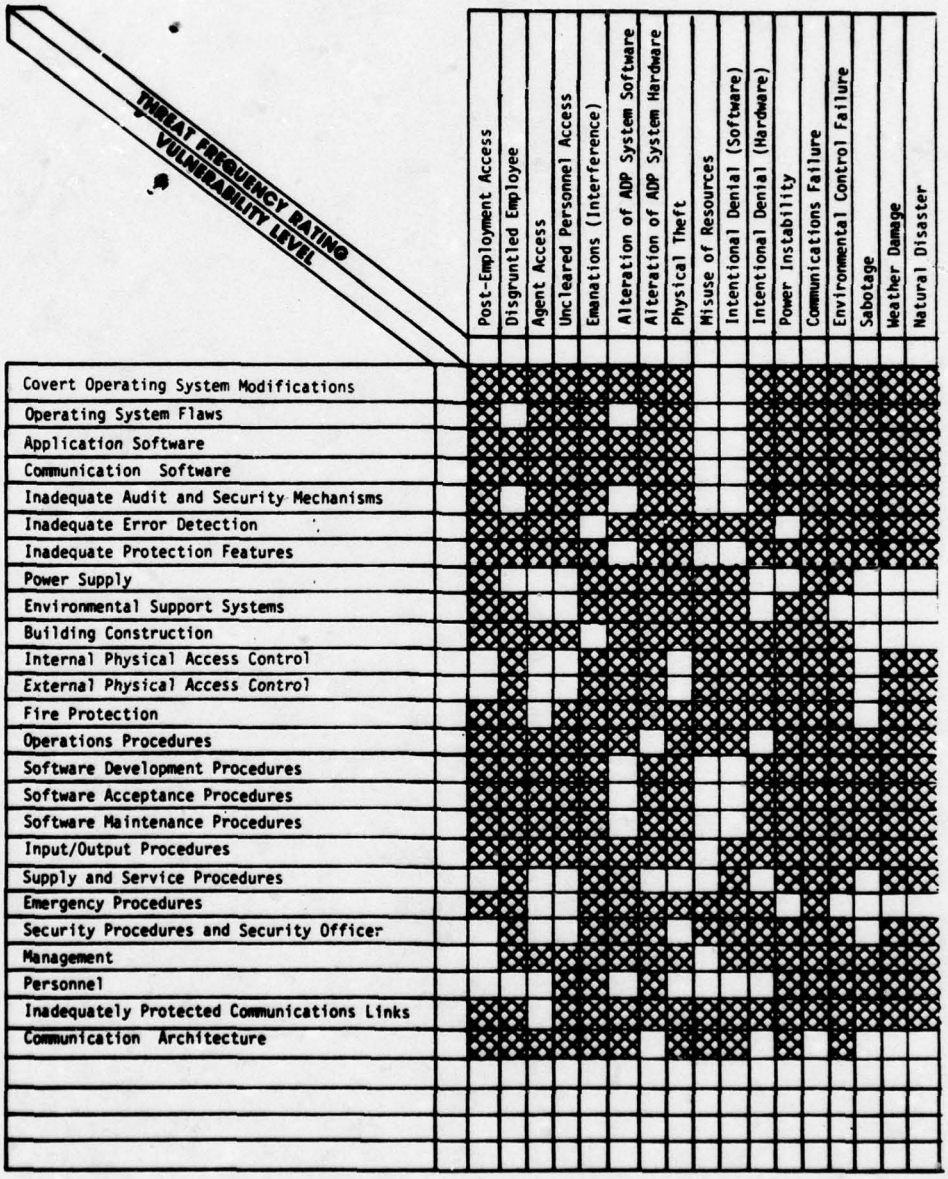


Figure _-67

Table _-6[D]. Estimation of Number of Successful Attacks

Vulnerability Level:	Threat Rating																							
	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8	8⁺
VL	0	0	0	0	0	0	0	0	0	0	0	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1	1	1
L	0	0	0	0	1⁻	1⁻	1	1⁺	1⁺	1⁺	2⁻	2⁻	2⁻	2	2	2	2⁺	2⁺	2⁺	2⁺	3⁻	3⁻	3⁻	3
M	0	1⁻	1⁻	1	1	1⁺	2⁻	2	2	2	2⁺	2⁺	3⁻	3⁻	3⁻	3	3	3⁺	4⁻	4	4⁺	5⁻	5	5
H	1⁻	1	1⁺	2⁻	2	2	2⁺	3⁻	3	3⁺	4⁻	4	4	4⁺	5	5	5⁺	6⁻	6	6⁺	7⁻	7	7	7⁺
VH	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8	8⁺

Instructions: Ignore the precision portion of the threat rating. Locate the row and column marked with the appropriate vulnerability level and threat rating. The rating for the estimate of the number of times that the threat exploits the vulnerability is found at the intersection of the row and column.

(1) For each threat listed on a threat/vulnerability form, transfer the threat rating from the Threat Tally Sheet to the first row of the matrix.

(2) For each vulnerability listed on the threat/vulnerability form, transfer the vulnerability level from the Vulnerability Tally Sheet to the first column of the matrix.

(3) For each applicable threat/vulnerability pair (threats and vulnerabilities which are not related for an impact have been removed from consideration), use Table _-6[D] to estimate the number of times that the particular threat will exploit the particular vulnerability. Place this value at the intersection of the row and column.

(4) Extra rows and columns have been provided to add additional vulnerabilities and threats identified in the threat and vulnerability analyses. List only threats that could have the indicated impact on a threat/vulnerability merger form. Do not consider threat and vulnerability pairs that are not related.

1.4.6 Asset Exposure Analysis Procedure. In this step all asset exposure computations are performed.

a. Analysis of the Impact of Threats on Non-Dollar-Valued Assets.

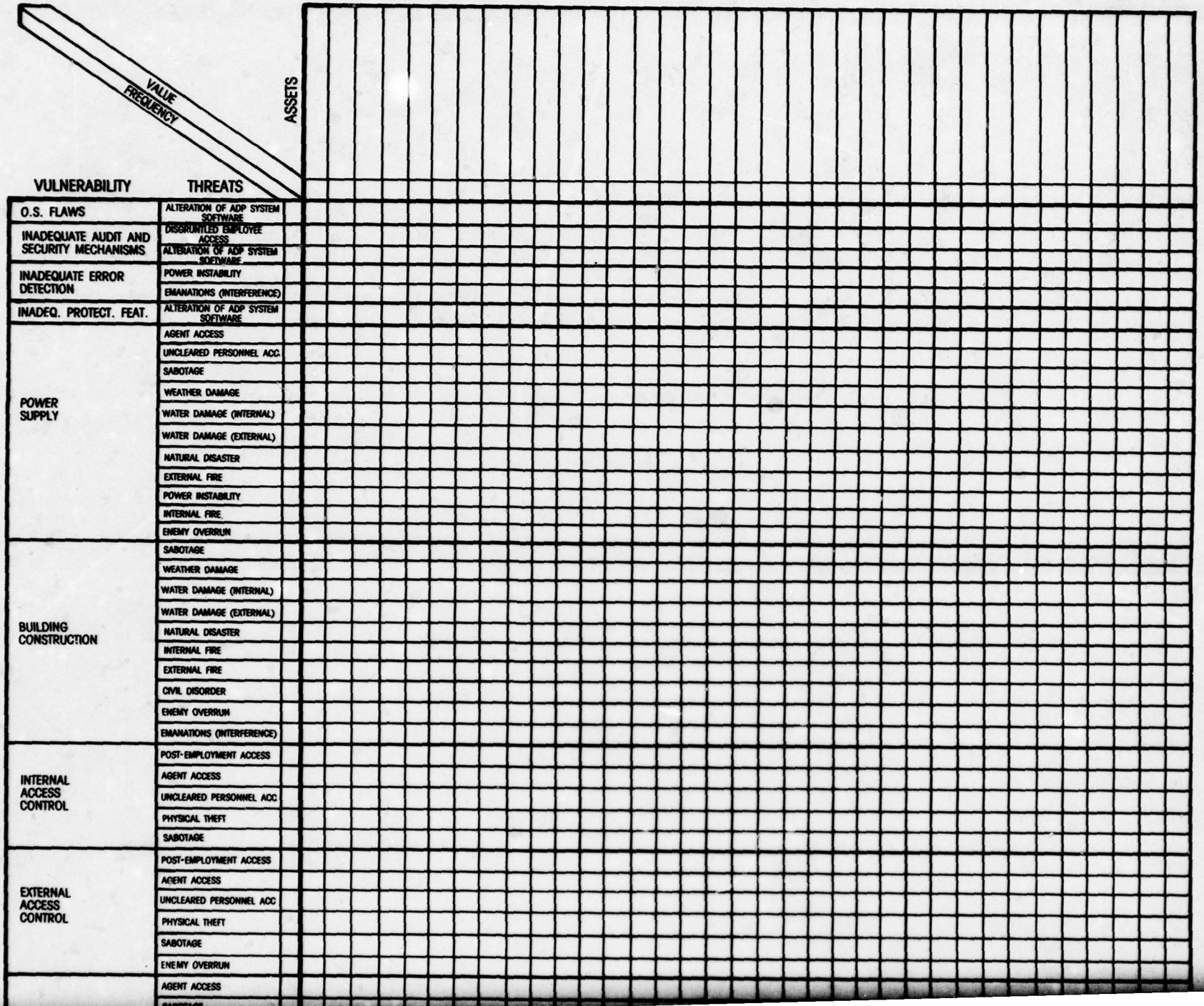
(1) Forms and Tables Required.

(a) Completed asset evaluation forms.

(b) Completed threat/vulnerability merger forms for destruction, disclosure, modification, and denial of service.

(c) Preprinted asset exposure forms (Figures _-68 through _-71) for:

IMPACT CATEGORY: DESTRUCTION
ASSET TYPE: NON-DOLLAR-VALUED



FIRE PROTECTION	INTERNAL FIRE
	EXTERNAL FIRE
	DISGRUNTLED EMPLOYEE
	UNCLEARED PERSONNEL
	ENEMY OVERRUN
OPERATIONS PROCEDURES	ALTERATION OF ADP SYSTEM HARDWARE
	DISGRUNTLED EMPLOYEE
	POWER INSTABILITY
SOFTWARE DEV. PROCED.	ALTERATION OF ADP SYSTEM SOFTWARE
	DISGRUNTLED EMPLOYEE
SOFTWARE ACC. PROCED.	ALTERATION OF ADP SYSTEM SOFTWARE
SOFTWARE MAINT. PROCED.	ALTERATION OF ADP SYSTEM SOFTWARE
	DISGRUNTLED EMPLOYEE
SUPPLY AND SERVICE PROCEDURES	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	UNCLEARED PERSONNEL ACC.
	PHYSICAL THEFT
	SABOTAGE
	DISGRUNTLED EMPLOYEE
	ALTERATION OF ADP SYSTEM HARDWARE
EMERGENCY PROCEDURES	AGENT ACCESS
	UNCLEARED PERSONNEL ACC.
	SABOTAGE
	WEATHER DAMAGE
	WATER DAMAGE (INTERNAL)
	WATER DAMAGE (EXTERNAL)
	NATURAL DISASTER
	INTERNAL FIRE
	EXTERNAL FIRE
	POWER INSTABILITY
	ENEMY OVERRUN
SECURITY PROCEDURES AND SECURITY OFFICER	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	ALTERATION OF ADP SYSTEM HARDWARE
	UNCLEARED PERSONNEL ACC.
	PHYSICAL THEFT
	SABOTAGE
MANAGEMENT	POST-EMPLOYMENT ACCESS
PERSONNEL	DISGRUNTLED EMPLOYEE ACC.
	AGENT ACCESS
	PHYSICAL THEFT
	POST-EMPLOYMENT ACCESS
	UNCLEARED PERSONNEL ACC.
COMMUNICATION ARCHITECTURE	SABOTAGE
	WEATHER DAMAGE
	WATER DAMAGE (INTERNAL)
	WATER DAMAGE (EXTERNAL)
	NATURAL DISASTER

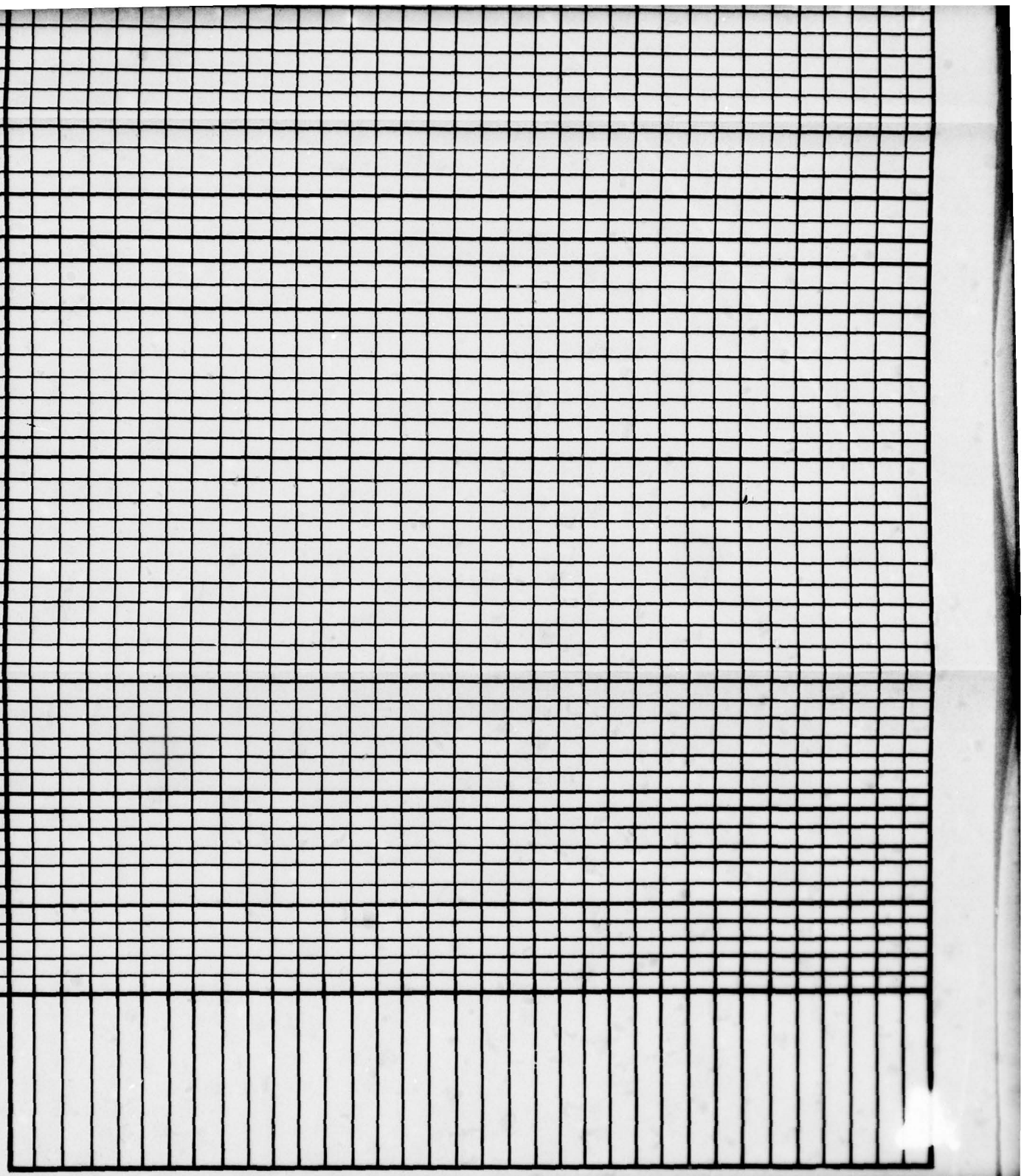
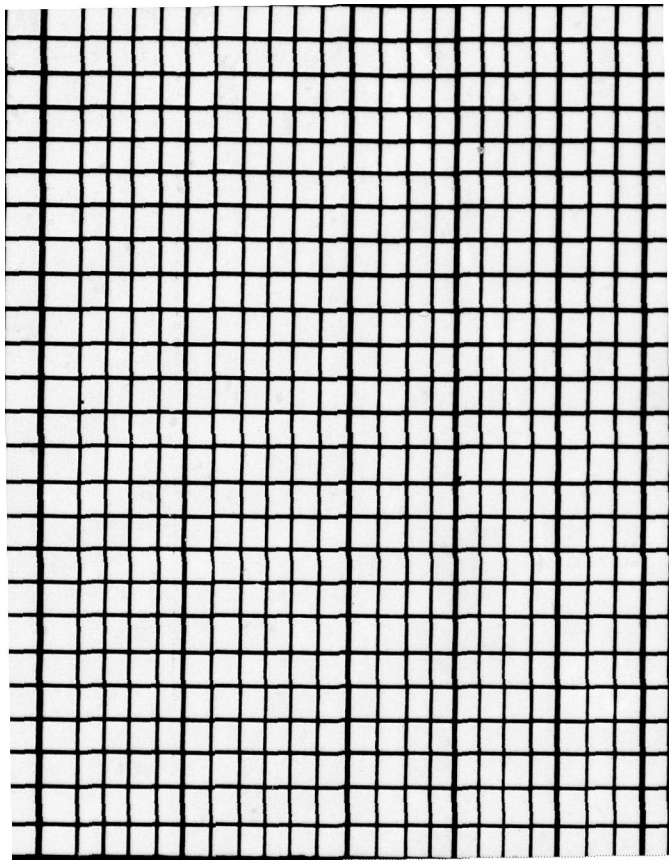
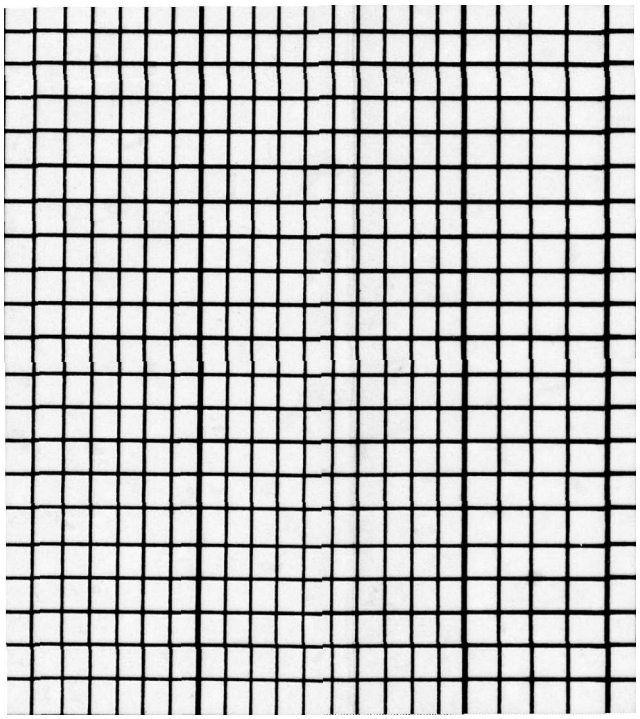


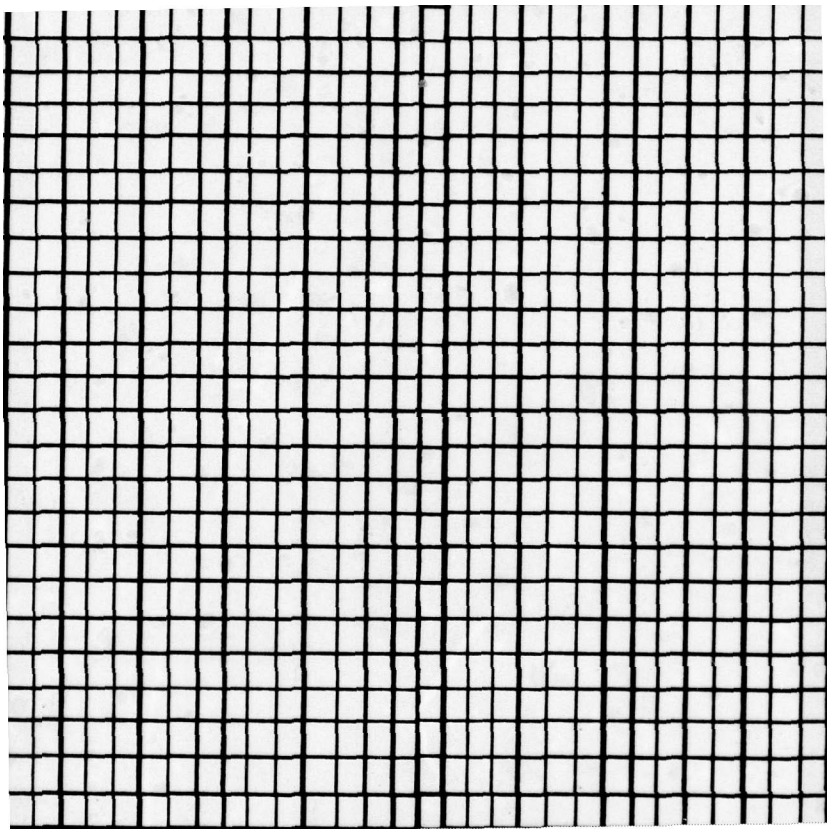
Figure -68. Asset Exposure





PERSONNEL	FRAUD	
	DISCLOSURE OF INFO	
	PHYSICAL THEFT	
	EAVESDROPPING	
	MISUSE OF RESOURCES	
	POST-EMPLOYMENT ACCESS	
INADEQUATELY PROTECTED COMMUNICATIONS LINKS	EMANATION (UNINTENTIONAL)	
	EMANATIONS (COVERT)	
	FRAUD	
	EAVESDROPPING	
COMMUNICATION ARCHITECTURE	ALTERATION OF ADP SYSTEM HARDWARE	
	FREQUENCY OF DISCLOSURE RATING FOR EACH ASSET	

Figure _-69. Asset Exposure

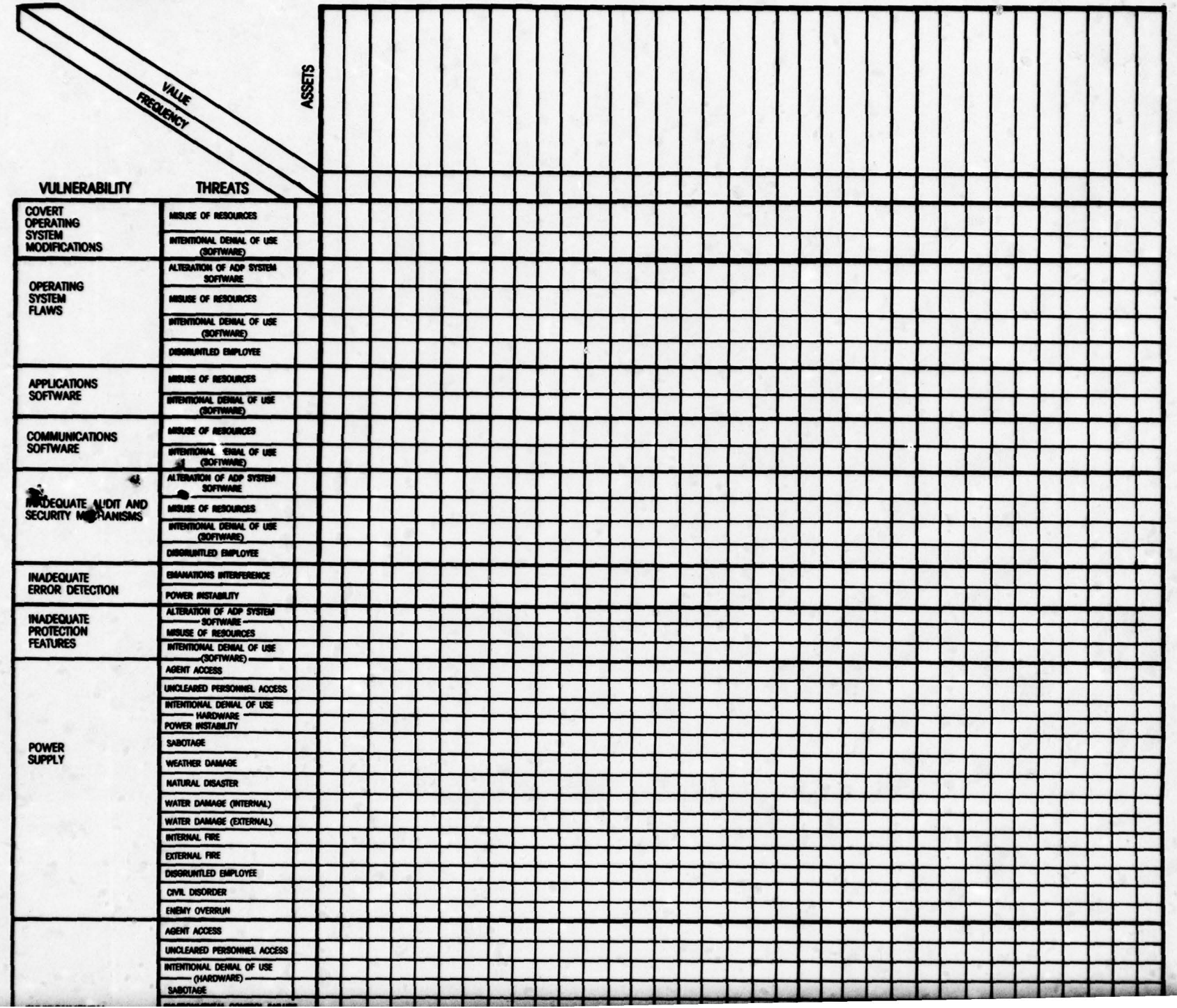


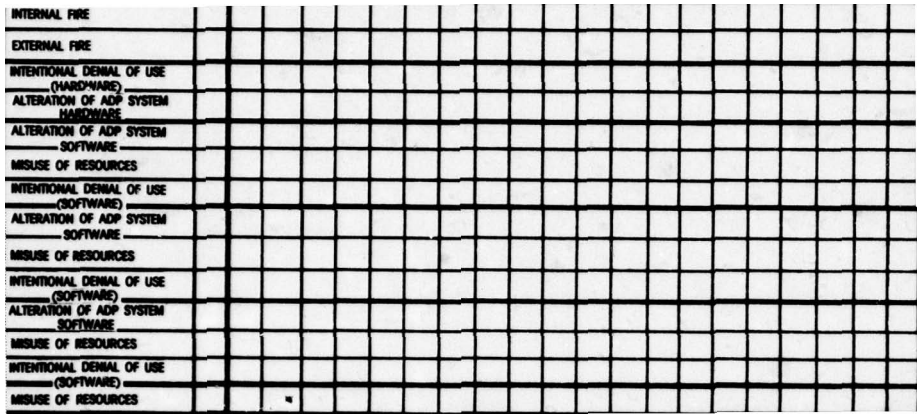
INADEQUATELY PROTECTED COMMUNICATONS LINKS	FRAUD	AGENT ACCESS	FRAUD

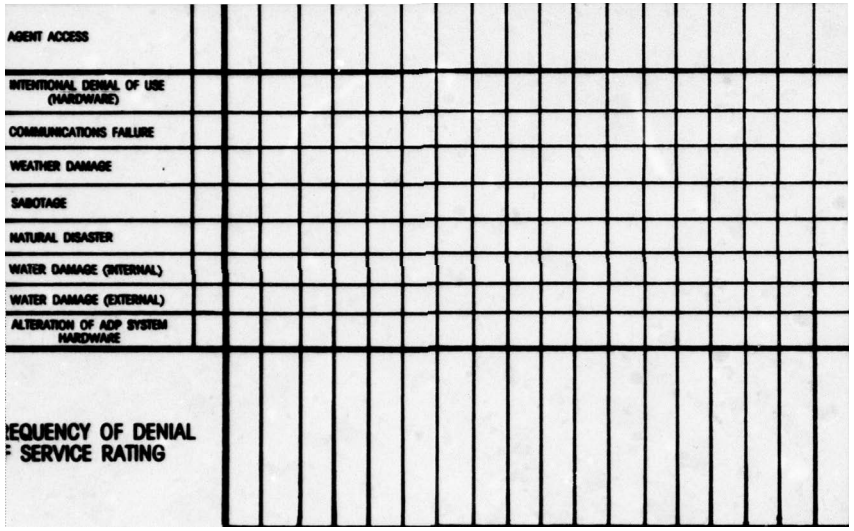
FREQUENCY OF MODIFICATION RATING FOR EACH ASSET

gure _-70. Asset Exposure

IMPACT CATEGORY: DENIAL OF SERVICE
ASSET TYPE: NON-DOLLAR-VALUED




INTERNAL FIRE
EXTERNAL FIRE
INTENTIONAL DENIAL OF USE (HARDWARE)
ALTERATION OF ADP SYSTEM HARDWARE
ALTERATION OF ADP SYSTEM SOFTWARE
MISUSE OF RESOURCES
INTENTIONAL DENIAL OF USE (SOFTWARE)
ALTERATION OF ADP SYSTEM SOFTWARE
MISUSE OF RESOURCES
INTENTIONAL DENIAL OF USE (SOFTWARE)
ALTERATION OF ADP SYSTEM SOFTWARE
MISUSE OF RESOURCES
INTENTIONAL DENIAL OF USE (SOFTWARE)
MISUSE OF RESOURCES


AGENT ACCESS
INTENTIONAL DENIAL OF USE (HARDWARE)
COMMUNICATIONS FAILURE
WEATHER DAMAGE
SABOTAGE
NATURAL DISASTER
WATER DAMAGE (INTERNAL)
WATER DAMAGE (EXTERNAL)
ALTERATION OF ADP SYSTEM HARDWARE
EQUENCY OF DENIAL
SERVICE RATING

1 Asset Type: Non-dollar-Valued

2 Impact Categories: Destruction, Disclosure, Modification, Denial of Service, if no additional threats or vulnerabilities have been added.

Or, blank asset exposure forms (Figure _-72) if additional threats or vulnerabilities have been added. (Make extra copies of any blank forms used.)

(d) Tables _-1[D] and _-7[D]. (Make extra copies of Table _-7[D].)

(2) Procedure. Perform the following procedure for each of the four impact categories. If no threats or vulnerabilities have been added, begin with step b using the preprinted asset evaluation forms. Otherwise begin with step a using blank asset evaluation forms.

(a) If threats or vulnerabilities have been added, copy all of the vulnerabilities, along with all applicable threats, from the Threat/Vulnerability Merger Form for the impact category to a blank Asset Evaluation Form. Use the format of the preprinted asset evaluation forms as guidance.

(b) Enter the names of all assets listed on the Asset Evaluation Form as having non-dollar values for the impact category in the spaces allotted for assets on the Asset Exposure Form.

(c) Transfer the appropriate impact value for each asset from the Asset Evaluation Form to the appropriate box on the Asset Exposure Form.

(d) Transfer the frequency of successful attacks for each threat/vulnerability pair from the appropriate Threat/Vulnerability

BLANK ASSET EXPOSURE FORM

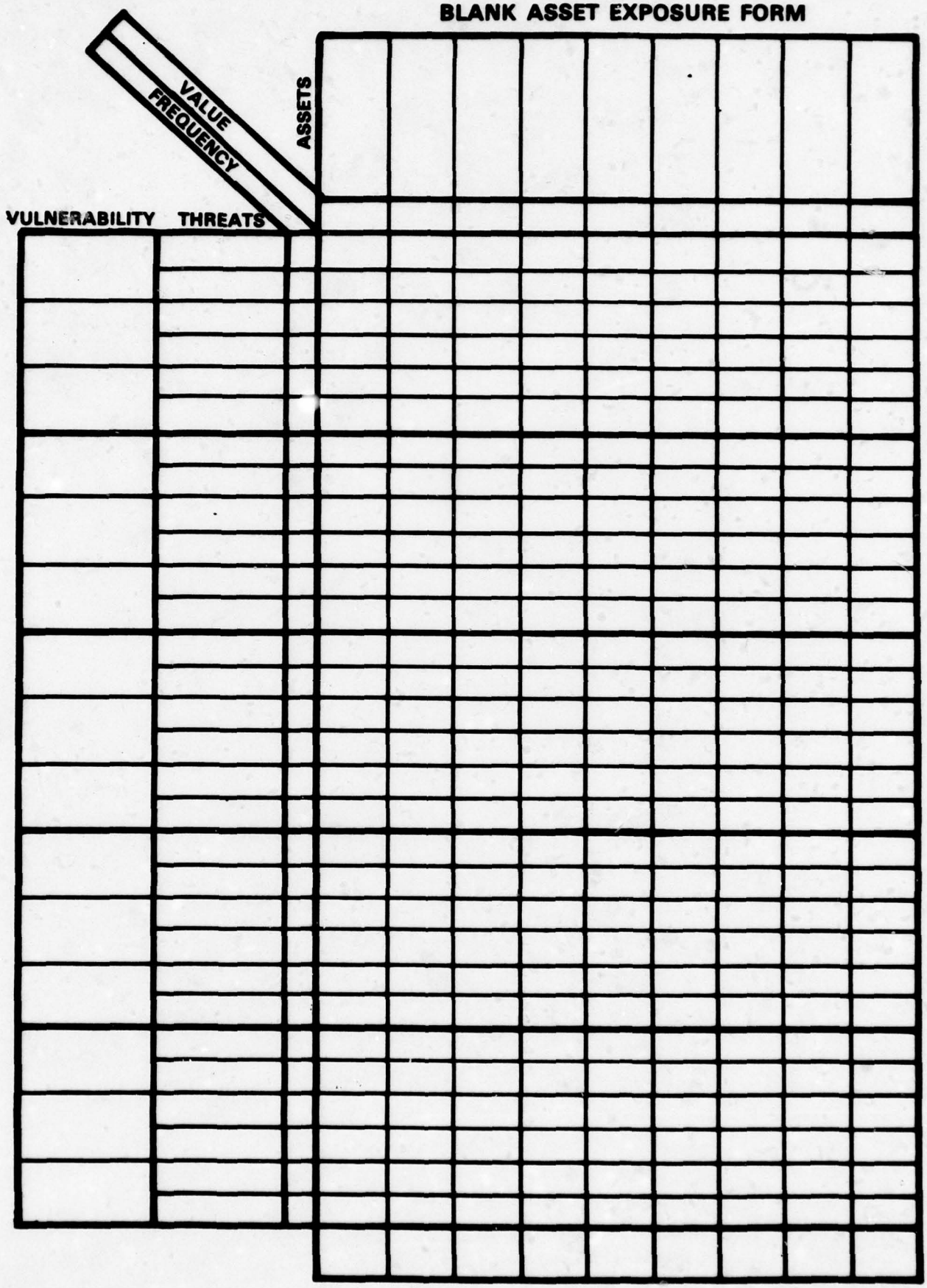


Figure _-72

Table _-1[D]. Frequency of Attacks

Frequency	Rating
Never	0
Once in 300 years	1
Once in 30 years	2
Once in 3 years	3
Once every 4 months or 3 times a year	4
Once a week or 52 times a year	5
Once a day or 365 times a year	6
Once every 2 hours	7
Once every 15 minutes	8

Note: Ratings may be modified by $^{+}$ for "more often than" or $^{-}$ for "less often than." For example, 3^{+} is more often than every 3 years and 3^{-} is less often than every 3 years.

ADDING FREQUENCY RATINGS

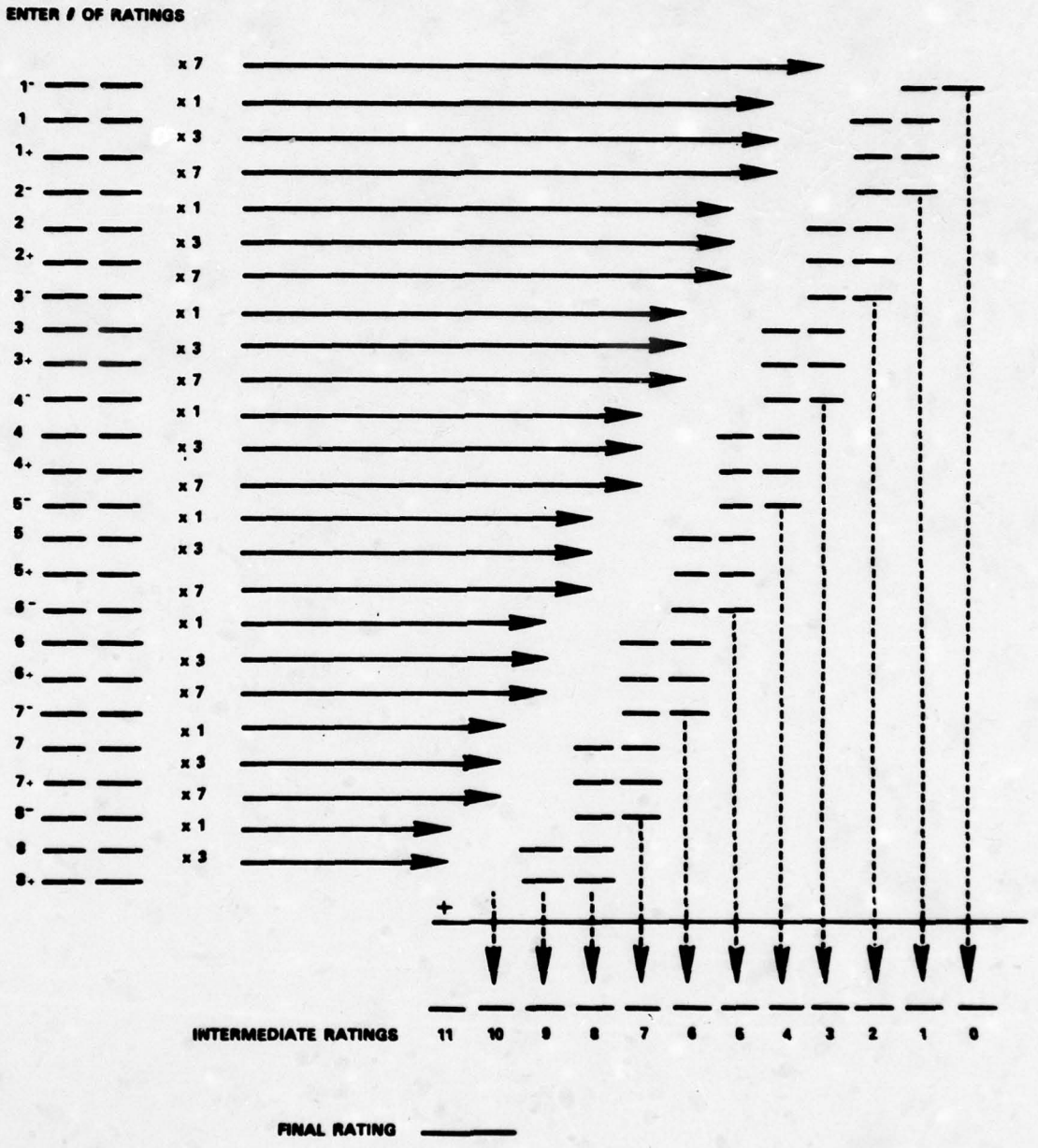


Table _-7[D]

INSTRUCTIONS FOR USING TABLE _-7[D]

Use. Table _-7[D] is used to add either attack frequencies or asset exposures. Make copies of the table and do the computations directly on the table.

Instruction. The following instructions apply for the addition of attack-frequency ratings and the addition of asset-exposure ratings.

1. Enter in the number of ratings column the number of times each rating appears in the list to be added.

2. Multiply each line by the factor shown and enter the resulting number in the rightmost column, one digit per space.

3. Add the numbers in the rightmost column and enter the sum directly below, one digit per space.

4. The number of the leftmost space in this sum with a non-zero value will be the intermediate rating. Call the number of this column "n."

5. To compute the final rating, use the following guides:

Entry in the Leftmost Non-Zero Space	Final Rating
1	(n)
2, 3, 4	(n) +
5, 6, 7	(n+1)
8, 9	(n+1)

The final rating will be a successful attack frequency rating.

Merger Form to the corresponding box on the Asset Exposure Form.

(e) For every threat/vulnerability pair listed on the Asset Exposure Form, determine whether the given threat could have the indicated impact on each asset. If the threat could have that impact on the asset, enter the frequency rating into the box in the same row and column as the threat/vulnerability pair and the asset. Otherwise enter N/A (Not Applicable).

(f) For each asset listed on the Asset Exposure Form, add the ratings in the column using Table _-7([D] and enter the result in the box provided at the bottom of the column. Be sure to add the ratings from all pages of the form. This number represents the rating of the expected frequency of successful attacks having the specified impact on the asset. Use Table _-1[D] to convert this rating to an estimate of the actual frequency.

b. Analysis of the Impact of Threats on Dollar-Valued Assets.

(1) Forms Required.

(a) Completed asset evaluation forms.

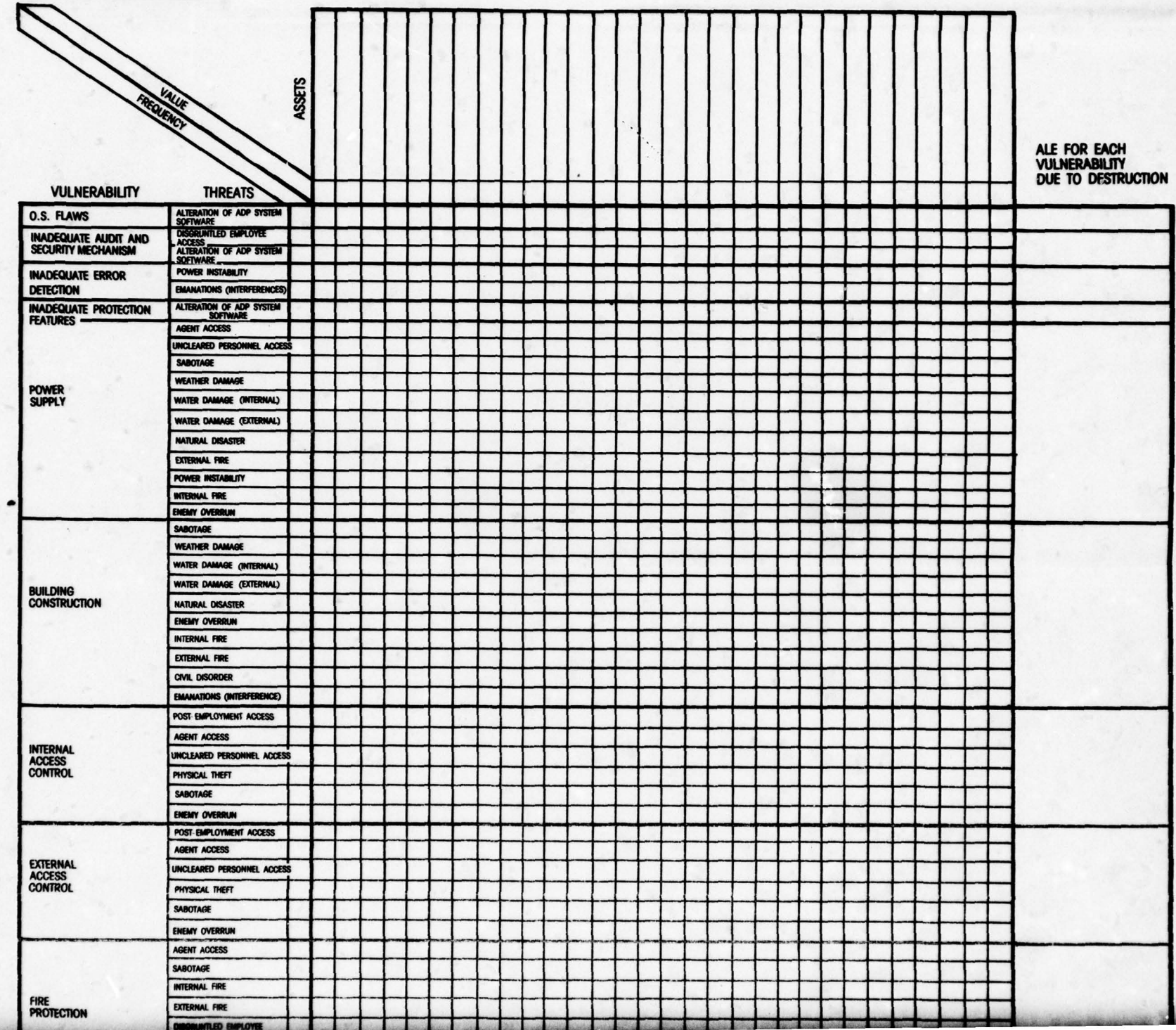
(b) Completed Threat/Vulnerability Merger Form for Destruction, Disclosure, Modification, and Denial of Service.

(c) Preprinted asset exposure forms (Figures _-73 through _-76) for:

1 Impact Category: Destruction, Disclosure, Modification, and Denial of Service.

2 Asset Type: Dollar-Valued.

IMPACT CATEGORY: DESTRUCTION
ASSET TYPE: DOLLAR-VALUED



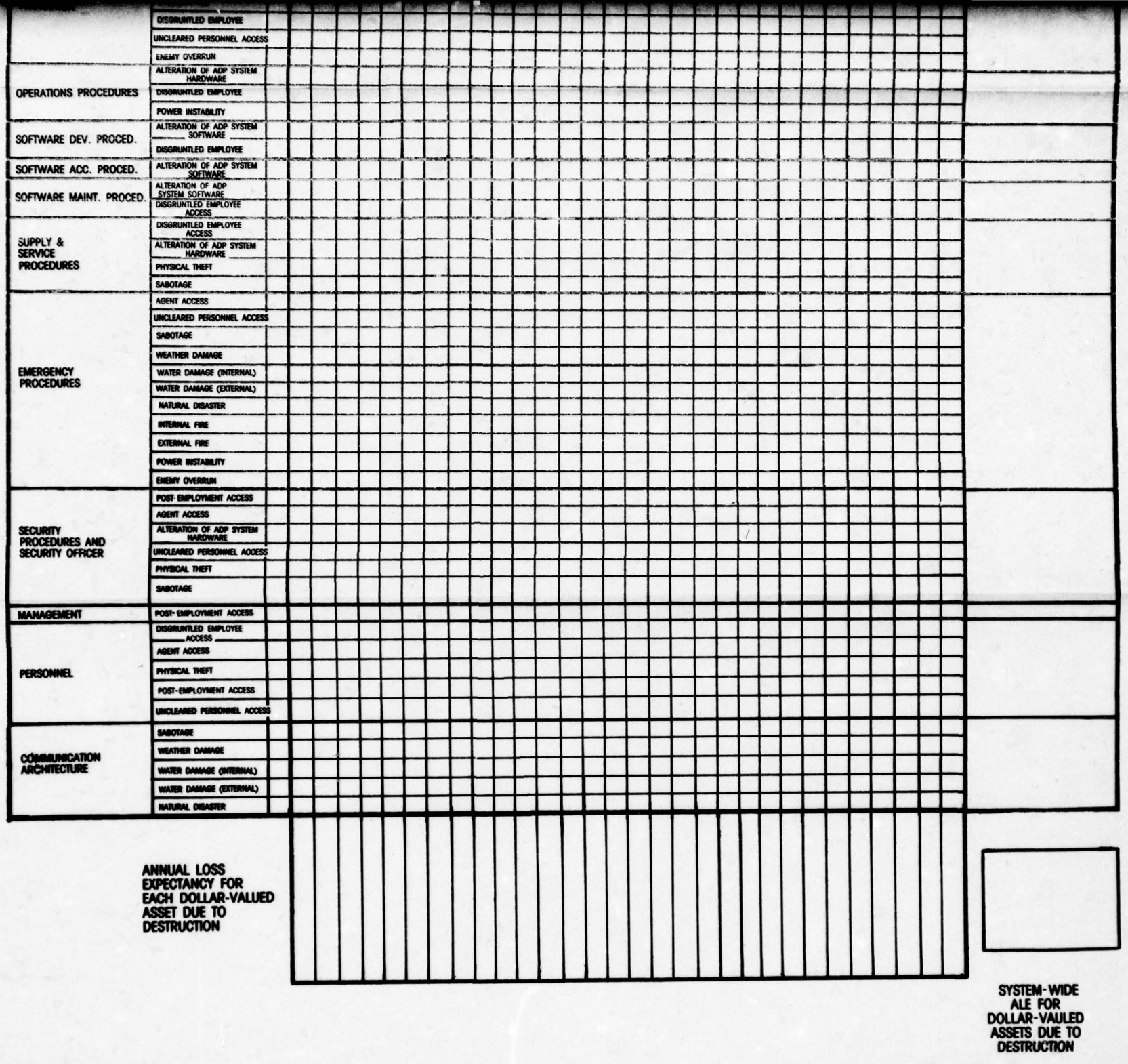
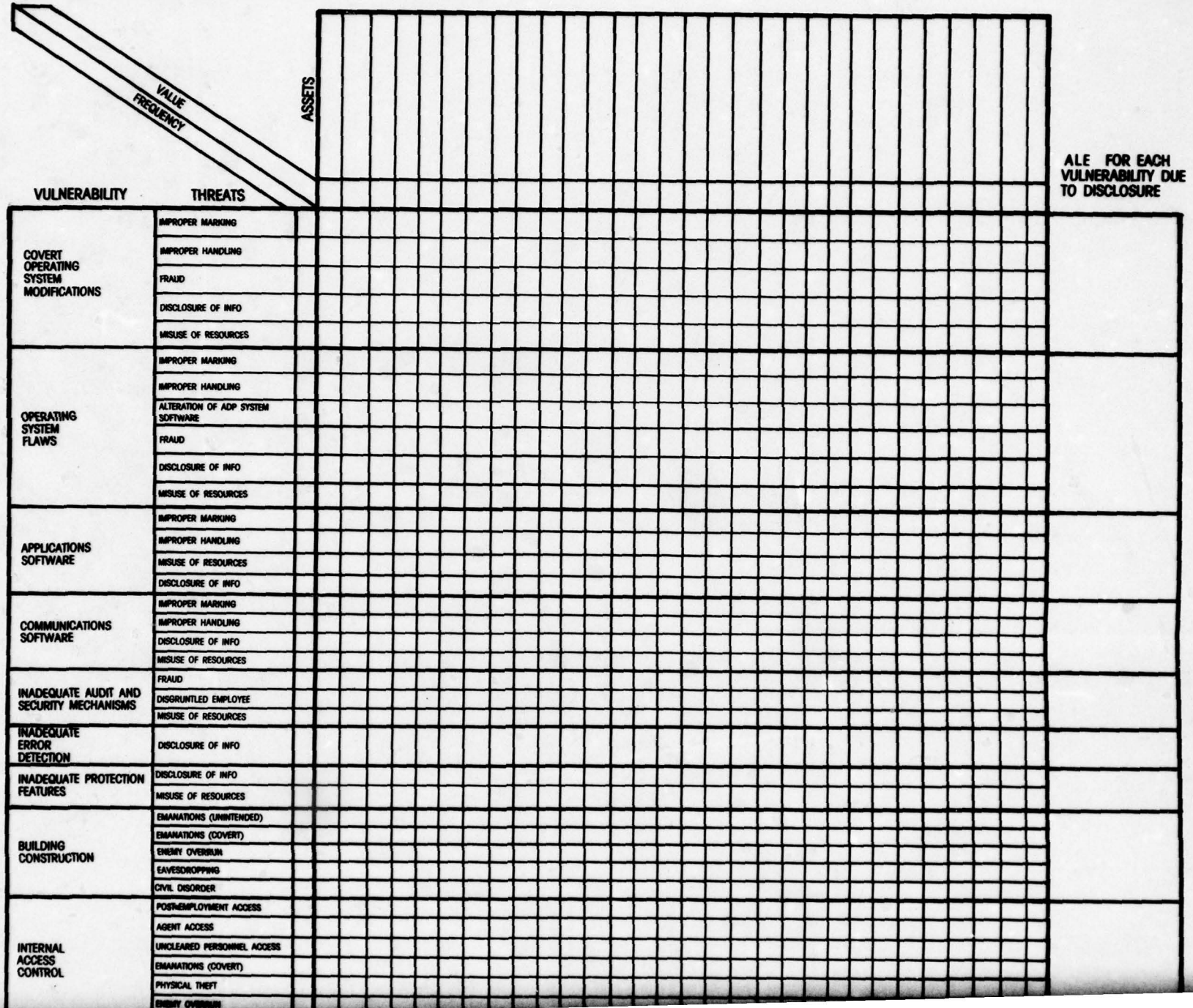


Figure -73. Asset Exposure

IMPACT CATEGORY: DISCLOSURE
ASSET TYPE: DOLLAR-VALUED



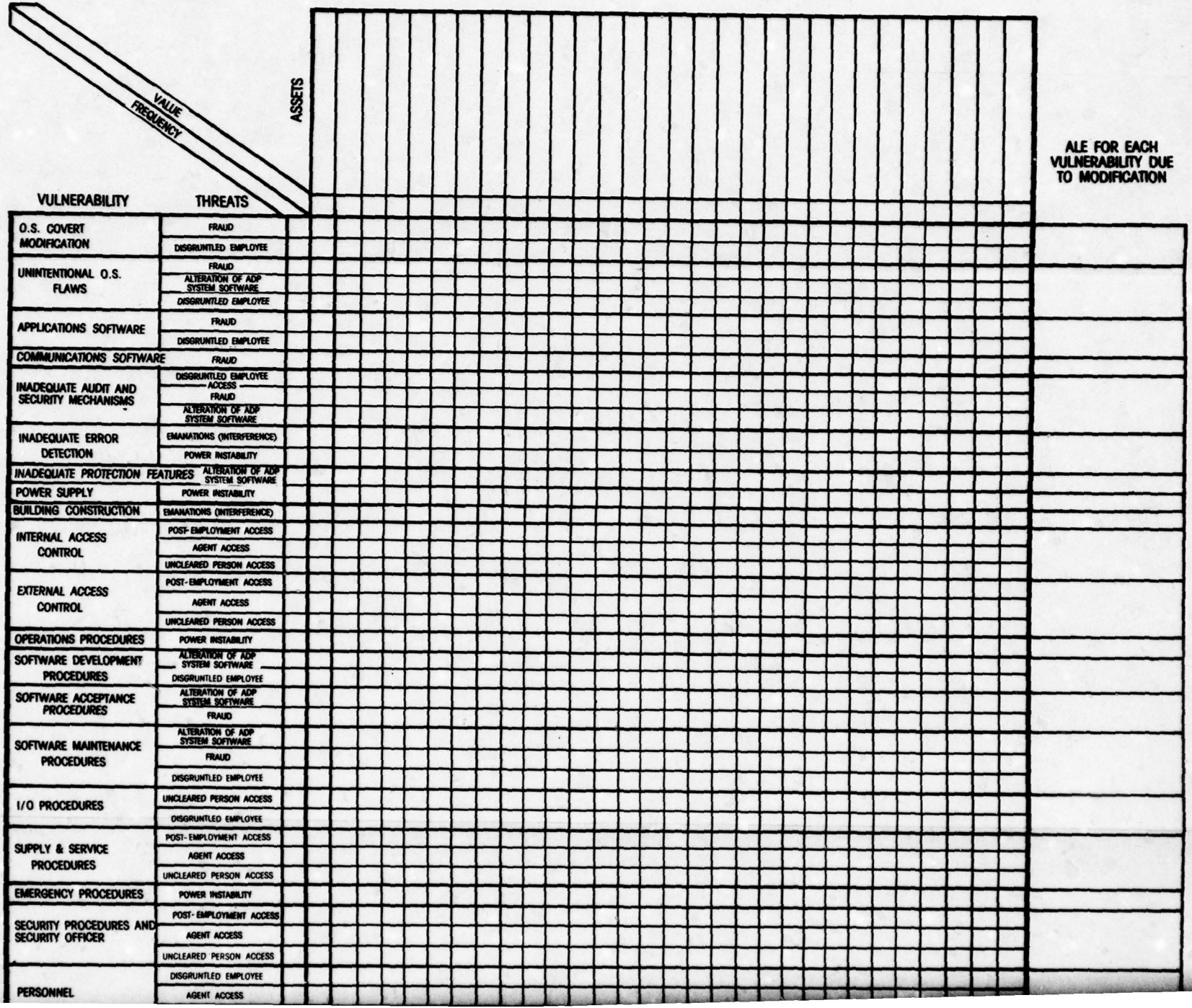
	ENEMY OVERRUN
	EAVESDROPPING
EXTERNAL ACCESS CONTROL	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	ENEMY OVERRUN
	UNCLEARED PERSONNEL ACCESS
	EMANATIONS (COVERT)
	PHYSICAL THEFT
	EAVESDROPPING
	CIVIL DISORDER
OPERATIONS PROCEDURES	ALTERATION OF ADP SYSTEM HARDWARE
	IMPROPER HANDLING
	DISCLOSURE OF INFO
SOFTWARE DEVELOPMENT PROCESS	ALTERATION OF ADP SYSTEM SOFTWARE
	DISCLOSURE OF INFO
	MISUSE OF RESOURCES
SOFTWARE ACCEPTANCE PROCEDURES	ALTERATION OF ADP SYSTEM
	DISCLOSURE OF INFO
	MISUSE OF RESOURCES
SOFTWARE MAINTENANCE PROCEDURES	FRAUD
	ALTERATION OF ADP SYSTEM SOFTWARE
	DISCLOSURE OF INFO
	MISUSE OF RESOURCES
I/O PROCEDURES	UNCLEARED PERSONNEL ACCESS
	IMPROPER MARKING
	IMPROPER HANDLING
	POST-EMPLOYMENT ACCESS
	DISGRUNTLED EMPLOYEE
	EAVESDROPPING
	DISCLOSURE OF INFORMATION
SUPPLY AND SERVICE PROCEDURES	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	UNCLEARED PERSONNEL ACCESS
	EMANATIONS (COVERT)
	IMPROPER HANDLING
	ALTERATION OF ADP SYSTEM HARDWARE
	DISCLOSURE OF INFO
	PHYSICAL THEFT
	EAVESDROPPING
	MISUSE OF RESOURCES
EMERGENCY PROCEDURES	AGENT ACCESS
	UNCLEARED PERSONNEL ACCESS
	ENEMY OVERRUN
	DISCLOSURE OF INFO
SECURITY PROCEDURES AND SECURITY OFFICER	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	UNCLEARED PERSONNEL ACCESS
	EMANATIONS (UNINTENDED)
	EMANATIONS (COVERT)
	IMPROPER MARKING
	IMPROPER HANDLING
	ALTERATION OF ADP SYSTEM HARDWARE
	ENEMY OVERRUN
	DISCLOSURE OF INFO
	PHYSICAL THEFT
	EAVESDROPPING
	POST-EMPLOYMENT ACCESS

	EAVESDROPPING	
MANAGEMENT	POST-EMPLOYMENT ACCESS	
	IMPROPER HANDLING	
	MISUSE OF RESOURCES	
PERSONNEL	DISGRUNTLED EMPLOYEE ACCESS	
	IMPROPER MARKING	
	IMPROPER HANDLING	
	FRAUD	
	POST-EMPLOYMENT ACCESS	
	DISCLOSURE OF INFO	
	PHYSICAL THEFT	
	EAVESDROPPING	
	MISUSE OF RESOURCES	
INADEQUATELY PROTECTED COMMUNICATIONS LINKS	EMANATIONS (UNINTENDED)	
	EMANATIONS (COVERT)	
	FRAUD	
	EAVESDROPPING	
COMMUNICATION ARCHITECTURE	ALTERATION OF ADP SYSTEM HARDWARE	
FREQUENCY OF DISCLOSURE RATING FOR EACH ASSET		

SYSTEM-WIDE ALE ASSETS DUE TO DISCLOSURE

Figure _-74. Asset Exposure

IMPACT CATEGORY: MODIFICATION
ASSET TYPE: DOLLAR-VALUED



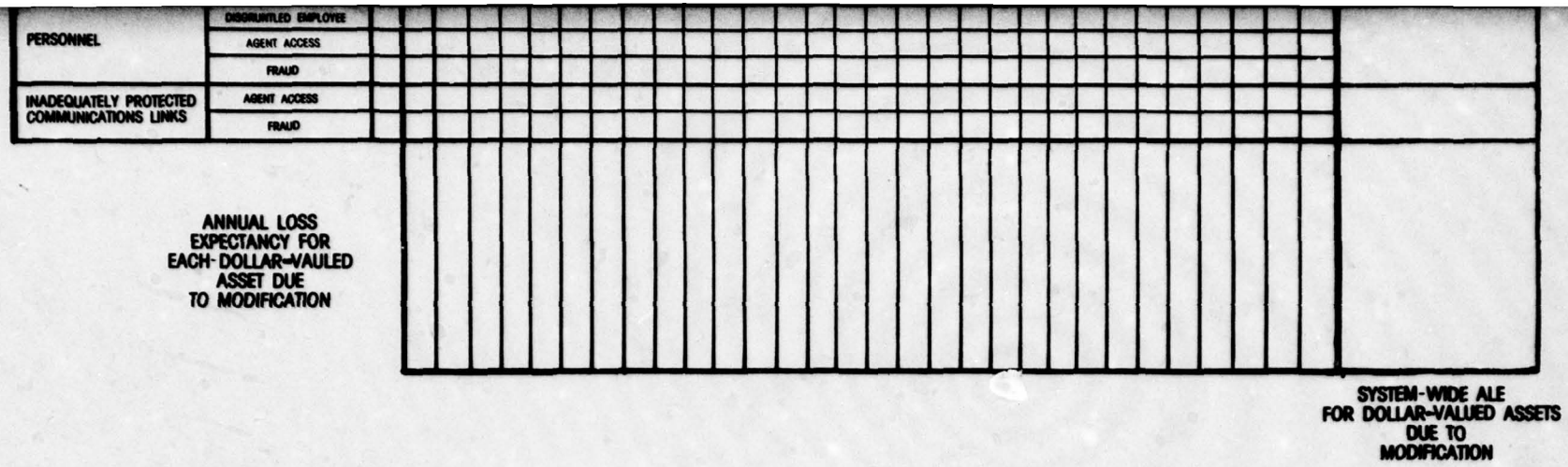
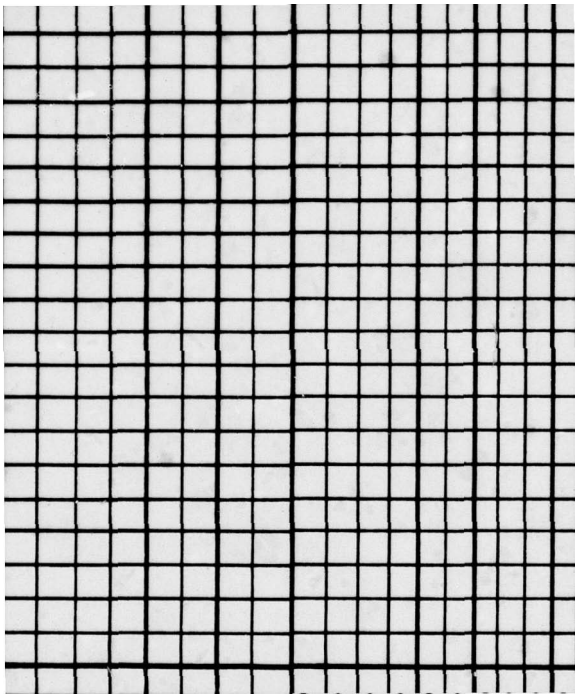


Figure _-75. Asset Exposure



	FAILURE
ENVIRONMENTAL SUPPORT SYSTEM	SABOTAGE
	ENEMY OVERRUN
	INTERNAL FIRE
	WEATHER DAMAGE
	NATURAL DISASTER
	WATER DAMAGE (INTERNAL)
	WATER DAMAGE (EXTERNAL)
	EXTERNAL FIRE
INTERNAL ACCESS CONTROL	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	UNCLEARED PERSONNEL ACCESS
	PHYSICAL THEFT
	ENEMY OVERRUN
	SABOTAGE
EXTERNAL ACCESS CONTROL	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	UNCLEARED PERSONNEL ACCESS
	ENEMY OVERRUN
	PHYSICAL THEFT
	SABOTAGE
FIRE PROTECTION	AGENT ACCESS
	SABOTAGE
	ENEMY OVERRUN
	INTERNAL FIRE
	EXTERNAL FIRE
OPERATIONS PROCEDURES	INTENTIONAL DENIAL OF USE (HARDWARE)
	ALTERATION OF ADP SYSTEM (HARDWARE)
SOFTWARE DEVELOPMENT PROCEDURES	ALTERATION OF ADP SYSTEM (SOFTWARE)
	MISUSE OF RESOURCES
	INTENTIONAL DENIAL OF USE (SOFTWARE)
SOFTWARE ACCEPTANCE PROCEDURES	ALTERATION OF ADP SYSTEM (SOFTWARE)
	MISUSE OF RESOURCES
	INTENTIONAL DENIAL OF USE (SOFTWARE)
SOFTWARE MAINTENANCE PROCEDURES	ALTERATION OF ADP SYSTEM (SOFTWARE)
	MISUSE OF RESOURCES
	INTENTIONAL DENIAL OF USE (SOFTWARE)
I/O PROCEDURES	MISUSE OF RESOURCES
SUPPLY & SERVICE PROCEDURES	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	ALTERATION OF ADP SYSTEM (HARDWARE)
	UNCLEARED PERSONNEL ACCESS
	PHYSICAL THEFT
	MISUSE OF RESOURCES
	INTENTIONAL DENIAL OF USE (HARDWARE)
	SABOTAGE
EMERGENCY PROCEDURES	AGENT ACCESS
	UNCLEARED PERSONNEL ACCESS
	POWER INSTABILITY
	ENVIRONMENTAL CONTROL FAILURE
	SABOTAGE
	WEATHER DAMAGE
	NATURAL DISASTER
	ENEMY OVERRUN
	WATER DAMAGE (INTERNAL)
	WATER DAMAGE (EXTERNAL)
	INTERNAL FIRE
	EXTERNAL FIRE

	EXTERNAL FIRE
SECURITY PROCEDURES	POST-EMPLOYMENT ACCESS
	AGENT ACCESS
	UNCLEARED PERSONNEL ACCESS
	PHYSICAL THEFT
	SABOTAGE
MANAGEMENT	POST-EMPLOYMENT ACCESS
	MISUSE OF RESOURCES
PERSONNEL	DISGRUNTLED EMPLOYEE ACCESS
	AGENT ACCESS
	ALTERATION OF ADP SYSTEM SOFTWARE
	POST-EMPLOYMENT ACCESS
	PHYSICAL THEFT
	MISUSE OF RESOURCES
	INTENTIONAL DENIAL OF USE (SOFTWARE)
	INTENTIONAL DENIAL OF USE (HARDWARE)
INADEQUATE PROTECTION COMMUNICATION LINKS	AGENT ACCESS
COMMUNICATION ARCHITECTURE	INTENTIONAL DENIAL OF USE (HARDWARE)
	COMMUNICATIONS FAILURE
	WEATHER DAMAGE
	ALTERATION OF ADP SYSTEM (HARDWARE)
	WATER DAMAGE (INTERNAL)
	SABOTAGE
	NATURAL DISASTI
	WATER DAMAGE (EXTERNAL)

ANNUAL LOSS EXPECTANCY FOR EACH VULNERABILITY DUE TO DENIAL OF SERVICE

SYSTEM-WIDE ANNUAL LOSS EXPECTANCY FOR DOLLAR-VALUED ASSETS DUE TO DENIAL OF SERVICE

Figure _-76. Asse Exposure

3

Use the preprinted forms if no additional threats or vulnerabilities have been added.

Use blank asset evaluation exposure forms (Figure _-72), if additional threats or vulnerabilities have been added. Make extra copies of any blank forms used.

(d) Tables _-8[D] and _-9[D]. (Make extra copies of Table _-9[D]).

(2) Procedure. Perform the following procedure for each of the four impact categories.

(a) If threats or vulnerabilities have been added, copy all of the vulnerabilities, along with all the applicable threats, from the Threat/Vulnerability Merger Form for the same impact area to the blank Asset Exposure Form. Use the format of the preprinted asset evaluation forms as guidance.

If threats or vulnerabilities have been added, begin at step (a) using blank asset evaluation forms. Otherwise, begin at step (b) using the preprinted asset evaluation forms.

(b) Enter the name of each asset listed on the Asset Evaluation Form as having a dollar value in the impact category into the space allotted for assets on the Asset Exposure Form.

(c) Transfer the dollar value in the impact category from the Asset Evaluation Form to the appropriate box on the Asset Exposure Form for each asset identified in (b).

(d) Transfer the frequency of successful attack for each threat/vulnerability pair from the appropriate Threat/Vulnerability Merger Form to the corresponding box on the Asset Exposure Form.

Table _-8.[D] Average Asset Exposure Computation

Frequency of Successful Attacks

	1^-	1	1^+	2^-	2	2^+	3^-	3	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+
1^-										1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+
1									1	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6
1^+									1	1^+	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6
2^-							1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+	6^-	6^-	6^+
2						1	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7
2^+						1	1^+	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6	6^+	6^+	7
3^-				1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+	6^-	6^-	6^+	7^-	7^-	7^+
3			1	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8
3^+			1	1^+	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6	6^+	6^+	7	7^+	7^+	8
4^-	1^-	1^-	1^+	2^-	2^-	2^+	3^-	3^-	3^+	4^-	4^-	4^+	5^-	5^-	5^+	6^-	6^-	6^+	7^-	7^-	7^+	8^-	8^-	8^+
4	1	1^+	2	2	2^+	3	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9
4^+	1^+	2^-	2	2^+	3^-	3	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9
5^-	1^+	2	2^+	2^+	3	3^+	3^+	4	4^+	4^+	5	5^+	5^+	6	6^+	6^+	7	7^+	7^+	8	8^+	8^+	9	9^+
5	2	3^-	3	3	4^-	4	4	5^-	5	5	6^-	6	6	7^-	7	7	8^-	8	8	9^-	9	9	10^-	10
5^+	2^+	3^-	3^+	3^+	4^-	4^+	4^+	5^-	5^+	5^+	6^-	6^+	6^+	7^-	7^+	7^+	8^-	8^+	8^+	9^-	9^+	9^+	10^-	10^-
6^-	3^-	3	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+
6	3	3^+	4	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9	9	9^+	10	10	10^+	
6^+	3^+	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+		
7^-	4^-	4	4^+	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+			
7	4	4^+	5	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9	9	9^+	10	10	10^+				
7^+	4^+	5^-	5^+	5^+	6^-	6^+	6^+	7^-	7^+	7^+	8^-	8^+	8^+	9^-	9^+	9^+	10^-	10^+	10^+					
8^-	5^-	5	5^+	6^-	6	6^+	7^-	7	7^+	8^-	8	8^+	9^-	9	9^+	10^-	10	10^+						
8	5	5^+	6	6	6^+	7	7	7^+	8	8	8^+	9	9	9^+	10	10	10^+							
8^+	5^+	6^-	6^+	6^+	7^-	7^+	7^+	8^-	8^+	8^+	9^-	9^+	9^+	10^-	10^+	10^+								

Note: Ignore precision estimates for average exposure ratings.

Table _-9[D]. Exposure Computation

Asset or Vulnerability Name: _____

Exposure Value	Number of Ratings:	x	Multiplier	=	Intermediate Value
1-	_____	x	7	=	_ _ _
1	_____	x	10	=	_,_ _ 0
1+	_____	x	30	=	_,_ _ 0
2-	_____	x	70	=	_,_ _ 0
2	_____	x	100	=	_ _,_ 0 0
2+	_____	x	300	=	_ _,_ 0 0
3-	_____	x	700	=	_ _,_ 0 0
3	_____	x	1,000	=	_ _ _,0 0 0
3+	_____	x	3,000	=	_ _ _,0 0 0
4-	_____	x	7,000	=	_ _ _,0 0 0
4	_____	x	10,000	=	_,_ _ 0,0 0 0
4+	_____	x	30,000	=	_,_ _ 0,0 0 0
5-	_____	x	70,000	=	_,_ _ 0,0 0 0
5	_____	x	100,000	=	_ _,_ 0 0,0 0 0
5+	_____	x	300,000	=	_ _,_ 0 0,0 0 0
6-	_____	x	700,000	=	_ _,_ 0 0,0 0 0
6	_____	x	1,000,000	=	_ _ _,0 0 0,0 0 0
6+	_____	x	3,000,000	=	_ _ _,0 0 0,0 0 0
7-	_____	x	7,000,000	=	_ _ _,0 0 0,0 0 0
7	_____	x	10,000,000	=	_,_ _ _,0 0 0,0 0 0
7+	_____	x	30,000,000	=	_,_ _ _,0 0 0,0 0 0
8-	_____	x	70,000,000	=	_,_ _ _,0 0 0,0 0 0
8	_____	x	100,000,000	=	_ _,_ _ _,0 0 0,0 0 0
8+	_____	x	300,000,000	=	_ _,_ _ _,0 0 0,0 0 0
			Total Dollar Value	$	_____

Instructions for Table -9[D]

1. For each Exposure Value, count the number of times the value appears in the row or column being considered on the Asset Exposure Form. Enter this number in the Number of Ratings column.
2. For each row multiply the number of ratings by its multiplier to obtain the Intermediate Value.
3. Add all of the intermediate values to obtain the Total Dollar Value.

(e) For every threat/vulnerability pair listed on the Asset Exposure Form, determine whether the threat could have the particular impact on <u>each</u> asset. If the threat could have that impact on the asset, use Table _-8[D] to compute the portion of the Annual Loss Estimate for the asset due to this threat/vulnerability pair. Enter this value into the box in the same row and column as the threat/vulnerability pair and the asset. Otherwise enter N/A (Not Applicable) in the box.

(f) For each asset listed on the Asset Exposure Form, use Table _-9[D] to add the ratings in the column. Enter the result in the box provided at the bottom of the column. Be sure to add the ratings from all pages of the form. This number is the Annual Loss Expectancy (ALE) in dollars from threats having the particular impact on the asset.

(g) Add the annual loss expectancies for all assets to get the system-wide annual loss expectancy from the impact category, and enter this in the box provided at the lower right.

c. <u>Computation of System-Wide Cost Measures</u>. This section develops the annual loss expectancy for the entire ADP facility and provides a breakdown of financial losses caused by each vulnerability of the facility.

(1) <u>Required Forms</u>.

(a) Completed asset exposure forms for:

<u>1</u> Asset Type: Dollar-Valued.

<u>2</u> Impact Categories: Destruction, Disclosure, Modification, and Denial of Service

(b) Blank Total Exposure Form (Figure _-77).

TOTAL EXPOSURE FORM

VULNERABILITY	TOTAL ANNUAL COST DUE TO VULNERABILITY
Covert Operating System Modifications	
Operatng System Flaws	
Application Software	
Communication Software	
Inadequate Auditors Security Mechanisms	
Inadequate Error Detection	
Inadequate Protection Features	
Power Supply	
Environmental Support Systems	
Building Construction	
Internal Access Control	
External Access Control	
Fire Protection	
Operations Procedures	
Software Development Procedures	
Software Acceptance Procedures	
Software Maintenance Procedures	
Input/Output Procedures	
Supply and Service Procedures	
Emergency Procedures	
Security Procedures and Security Office	
Management	

Figure _-77 (Page 1 of 2)

Total Exposure Form (Continued)

VULNERABILITY	TOTAL ANNUAL COST DUE TO VULNERABILITY
Personnel	
Inadequately Protected Communication Links	
Communication Architecture	

TOTAL SYSTEM-WIDE ANNUAL LOSS EXPECTANCY

Fiugre _-77 (Page 2 of 2)

(2) Procedure.

(a) For each vulnerability listed on the Total Exposure Form, add the total costs caused by that vulnerability from the four asset exposure forms. Enter this total in the box on the Total Exposure Form.

(b) Add the system-wide annual loss expectancy from the four asset exposure forms. Enter the sum in the total system-wide annual loss expectancy box on the Total Exposure Form.

1.4.7 Countermeasures Selection and Application Procedure. Countermeasures are applied for two reasons:

- To reduce asset exposure for dollar-valued assets
- To provide a required level of protection for non-dollar-valued assets

For a discussion of the method for selecting countermeasures, see paragraph 1.3.7.

Forms Required.

(1) Working copies of the Threat/Vulnerability Form--Disclosure.

(2) Working copies of the Threat/Vulnerability Form--Destruction.

(3) Working copies of the Threat/Vulnerability Form--Modification.

(4) Working copies of the Threat/Vulnerability Form--Denial of Service.

(5) Completed total exposure forms.

(6) All seven completed asset exposure forms.

(7) Tables _-10[D] and _-11 [D].

(8) The descriptions of countermeasures.

(9) Countermeasures Affecting Each Vulnerability (Figure _-78).

This procedure is divided into two interrelated parts: the selection of countermeasures and the application of countermeasures.

After you select a countermeasure for consideration by the procedure described in paragraph a, use the procedure described in paragraph b to determine the effect of applying the countermeasure. This will allow you to decide whether or not to implement the countermeasure.

a. Procedure for Countermeasure Selection. Follow this procedure in determining what countermeasures to use:

(1) Apply all countermeasures mandated by policy using the procedure outlined in paragraph b.

(2) Discard all countermeasures that would cost too much, would be ineffective at the particular ADP site, or are otherwise inappropriate.

(3) Apply all no-cost or low-cost countermeasures using the procedure outlined in paragraph b.

(4) Consider the cost-effectiveness of all countermeasures that are not already implemented or discarded.

To do this requires judgment on the part of the risk assessor, since it is generally impracticable to examine all possible combinations of the remaining countermeasures. The risk assessor should try representative

Table _-10[D]. Ratings for Countermeasures Application

Effectiveness of Countermeasures	Rating
Very High	VH
High	H
Medium	M
Low	L
Very Low	VL

Table _-11[D]. Countermeasures Effectiveness

Threat-Vulnerability Ratings

Countermeasure Effectiveness:	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8	8⁺
VL	0	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺	8⁻	8
L	0	0	1⁻	1	1⁺	2⁻	2	2⁺	3⁻	3	3⁺	4⁻	4⁻	4	4⁺	5⁻	5	5⁺	6⁻	6	6⁺	7⁻	7	7⁺
M	0	0	0	0	1⁻	1	1⁺	2⁻	2⁻	2⁻	2	2	2⁺	3⁻	3⁻	3	3	3⁺	4⁻	4	4⁺	5⁻	5	5
H	0	0	0	0	0	1⁻	1⁻	1	1⁺	1⁺	1⁺	2⁻	2⁻	2⁻	2	2	2	2⁺	2⁺	2⁺	2⁺	3⁻	3⁻	3
VH	0	0	0	0	0	0	0	0	0	0	0	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1⁻	1	1	1

Instructions: Ignore precision ratings. Locate the column containing the rating for the estimated number of successful attacks before the countermeasure is applied. Locate the row containing the rating for the effectiveness of the countermeasure. The rating for the estimated number of attacks which successfully penetrate the countermeasure is found at the intersection of the row and column.

VULNERABILITY	COUNTERMEASURES HAVING MAJOR EFFECT As Described in Sections of Appendix __	COUNTERMEASURES HAVING MINOR EFFECT As Described in Sections of Appendix __
Operating System Flaws (Intentional)	1.2.7, 1.2.9, 1.2.16, 1.2.17, 1.2.18, 1.3.5	1.2.3, 1.2.15
Operating System Flaws (Unintentional)	1.2.2, 1.2.3, 1.2.7, 1.2.10, 1.2.17, 1.2.18, 1.2.19, 1.3.5	1.2.1, 1.2.5
Application Software	1.2.3, 1.2.9	1.2.1, 1.2.5, 1.2.10, 1.2.17, 1.2.13
Communication Software	1.2.3, 1.2.9, 1.3.4	1.2.5, 1.2.10, 1.2.17, 1.2.13
Inadequate Audit and Security Mechanisms	1.2.1, 1.2.2, 1.2.4, 1.2.6, 1.2.8, 1.2.14, 1.2.19, 1.3.5 1.3.7, 1.8.2, 1.8.3, 1.8.4	1.2.5, 1.2.10, 1.2.17
Inadequate Error Detection	1.3.7	
Inadequate Protection Features	1.3.1, 1.3.2	
Hardware Configuration	1.2.12, 1.3.3, 1.3.6, 1.3.7, 1.8.5	
Power Supply	1.3.8	
Environmental Support Systems	1.7.3	
Building Construction	1.6.1, 1.6.2, 1.7.4, 1.8.5	

Figure _-78. Countermeasures Affecting Each Vulnerability (Page 1 of 3)

VULNERABILITY	COUNTERMEASURES HAVING MAJOR EFFECT As Described in Sections of Appendix __	COUNTERMEASURES HAVING MINOR EFFECT As Described in Sections of Appendix __
Internal Physical Access Control	1.6.1, 1.7.1	1.2.7
External Physical Access Control	1.6.1, 1.7.1	
Inadequate Fire Protection	1.7.2	
Operations Procedures	1.2.12, 1.3.3, 1.4.7	
Software Development Procedures	1.2.10, 1.2.15, 1.4.1	
Software Acceptance Procedures	1.2.5, 1.2.11, 1.2.13	1.2.9
Software Maintenance Procedures	1.2.9, 1.4.2, 1.2.11	1.2.15, 1.2.13
Input/Output Procedures	1.4.3	1.2.6, 1.2.7, 1.2.9, 1.2.14
Access Procedures	1.2.4, 1.4.4, 1.4.5, 1.6.2, 1.7.1	1.2.6, 1.2.19
Emergency Procedures	1.4.6	
Security Procedures and Security Office	1.4.8, 1.6.2	
Management	1.5.1	

Figure _-78. Countermeasures Affecting Each Vulnerability (Page 2 of 3)

VULNERABILITY	COUNTERMEASURES HAVING MAJOR EFFECT As Described in Sections of Appendix _	COUNTERMEASURES HAVING MINOR EFFECT As Described in Sections of Appendix _
Personnel	1.5.1	
Inadequately Protected Communication Links	1.3.4, 1.8.1, 1.8.6	
Communication Architecture	1.3.4, 1.3.6, 1.3.7, 1.8.6, 1.8.7	

Figure _-78. Countermeasures Affecting Each Vulnerability (Page 3 of 3)

samples of single countermeasures and groups of countermeasures selected by the following criteria:

(a) Select countermeasures that reduce the level of those vulnerabilities that are identified on the Total Exposure Form as having a large contribution to the total ALE. Countermeasures that are designed to correct a particular vulnerability are listed in Figure _-78 as having a major effect on that vulnerability. Countermeasures that have a small effect on the vulnerability as a side effect of correcting some other vulnerability are listed as having a minor effect on the vulnerability.

(b) Select countermeasures that are highly effective.

(c) Select countermeasures that affect more than one vulnerability.

(d) Select countermeasures that protect against the specific cause of a vulnerability.

Evaluate the countermeasures selected both singly and in combination to determine whether any of them are not cost-effective by themselves or whether they are not cost-effective in combination. A countermeasure that is not cost-effective by itself will not be cost-effective when applied in combination with other countermeasures.

The test for cost-effectiveness is made by applying the countermeasures as outlined in paragraph b and observing whether the reduction in the ALE is greater than the cost of the countermeasures. If so, the countermeasures are cost-effective.

(5) After you have applied all of the cost-effective countermeasures, examine the frequency of successful attacks against non-dollar-valued

assets on the four asset exposure forms for non-dollar-valued assets. If any of these assets are subjected to a risk that is unacceptable either by Navy policy or to the risk assessor, apply countermeasures to those vulnerabilities that allow the greatest number of attacks to succeed, in an attempt to lower the risk to an acceptable level.

b. Countermeasure Application. To determine the effect of a countermeasure or set of countermeasures, follow this procedure.

(1) Select a countermeasure or a set of countermeasures to be implemented as described in paragraph a.

(2) Evaluate the effectiveness of each of the selected countermeasures using Table _-10[D] on the following basis:

(a) The description of each countermeasure as found in Appendix ___ of the U.S. Navy ADP Handbook.

(b) The degree to which the safeguard will be compatible with the ADP system.

(c) The amount of duplication of protection that exists between the countermeasure under evaluation and other countermeasures being implemented or already in place in the ADP system. If countermeasures provide protection in different ways, this will have no effect on the rating. If the countermeasures duplicate each other in some way, the effectiveness rating of one of them will be reduced.

(d) If the countermeasure protects more than one vulnerability, make an effectiveness rating for each vulnerability.

(3) For each vulnerability that is protected by one or more countermeasures, modify all entries in the appropriate row of all four threat/

vulnerability merger forms using Table _-11[D]. If a vulnerability is affected by more than one countermeasure, modify that row once by each countermeasure.

(4) Perform the Asset Exposure Analysis (paragraph 1.4.6) using the modified threat/vulnerability merger forms.

1.4.8 Worst-Case Analysis Procedure (Optional). In this step, the effect of lack of precision in the threat and asset analyses can be determined.

a. Forms Required.

(1) Completed Threat Tally Sheet.

(2) Completed Vulnerability Tally Sheet.

(3) Blank threat/vulnerability merger forms for: destruction, disclosure, modification, denial of service.

(4) Blank asset exposure analysis forms for:

(a) Impact areas: destruction, disclosure, modification, denial of service.

(b) Asset types: dollar-valued and non-dollar-valued.

(5) Completed asset evaluation forms.

(6) Tables _-6[D], _-7[D], _-8[D], _-9[D], _-10[D], _-11[D], _-12[D].

b. Procedure.

(1) For each threat listed on the Threat Tally Sheet, use Table _-12[D] to estimate the maximum possible attack frequency from the threat rating shown.

Table _-12[D]. Estimate of Maximum Ratings

Precision Ratings

Frequency or Value Ratings	V	F	R
1^-	1^-	1	2
1	1	1^+	2^+
1^+	1^+	2^-	2^-
2^-	2^-	2	3
2	2	2^+	3^+
2^+	2^+	3^-	4^-
3^-	3^-	3	4
3	3	3^+	4^+
3^+	3^+	4^-	5^-
4^-	4^-	4	5
4	4	4^+	5^+
4^+	4^+	5^-	6^-
5^-	5^-	5	6
5	5	5^+	6^+
5^+	5^+	6^-	7^-
6^-	6^-	6	7
6	6	6^+	7^+
6^+	6^+	7^-	8^-
7^-	7^-	7	8
7	7	7^+	8^+
7^+	7^+	8^-	8^+
8^-	8^-	8	8^+
8	8	8^+	8^+
8^+	8^+	8^+	8^+

Directions: Locate the row with the frequency or asset rating for which the maximum value is to be computed. Locate the column with the precision of this rating. The maximum rating is at the intersection of the row and column.

(2) For each asset listed on the asset evaluation forms, use Table _-12[D] to estimate the largest possible value rating in each impact area where the asset has a dollar value.

(3) Perform the threat/vulnerability merger using the threat ratings computed in Step 1. Use the procedure in paragraph 1.4.5.

(4) Perform the asset exposure analysis using the asset ratings computed in Step 2. Use the procedure in paragraph 1.4.6.

c. Note. The ALEs and levels of risk computed in the worst-case analysis represent the least favorable view of the security at the ADP system or facility. Any countermeasures recommended as a result of this analysis must be considered with this in mind.

A worst-case analysis need only be done if a large number of ratings are rough, or if there are assets that require a particular level of protection and a test must be made to determine if the impression in some ratings means that this level is not being met.

ATTACHMENT -1

The Attachment contains an example of how the risk assessment forms are completed and interrelated. This example is not intended to provide complete instructions and should be used in conjunction with the step-by-step instructions provided earlier.

A rating with precision estimate is provided for each threat including installation specific threats. A sample form for the threat of Uncleared Personnel Access is provided in the sample information to justify the rating.

The Threat Tally Sheet contains the rating for this threat and for seven other threats. For brevity the threat evaluation forms for the other threats are not included.

A vulnerability level is provided for each vulnerability including installation specific vulnerabilities. A sample form for the vulnerability of Application Software is provided with sample information to justify the vulnerability level.

The Vulnerability Tally Sheet contains the vulnerability level for this vulnerability and for eleven other vulnerabilities. For brevity the vulnerabilities evaluation forms for the other vulnerabilities are not included.

The information from the Threat and Vulnerability Tally Sheets is transferred to the Threat/Vulnerability Merger Form. The form for modification is used as an example. The Frequency of Successful Attack is completed using the tables provided and entered at the insections of those threats and vulnerabilities that are not crossed out.

The information from the Threat/Vulnerability Merger Form is transferred to the Asset Exposure Form. This includes the Frequency of Successful Attack for each threat/vulnerability pair.

Assets are valued using the asset evaluation form. Different values can be provided for an asset depending upon the impact category being considered.

For this example values have been assigned to sample assets for unauthorized modification. Essentially these assets values are intended to represent the impact should threat asset be modified. High values have been assigned to the informational assets such as the payroll program indicating that the risk assesser believes the unauthorized modification of these assets would have a serious impact. The central processor also has a high impact value for unauthorized modification.

The threat/vulnerability pairs are then matched against the assets that could reasonably be impacted by a successful attack. The matching is accomplished on a judgmental basis considering each threat/vulnerability pair as a unique senario in regard to the asset being considered.

The summary information from the asset exposure form is transferred to the total exposure form for further analysis. In this case there are two major areas of vulnerability: Inadequate Audit and Security Mechanisms, and Application Software. At this point it may be advisable to evaluate the threat frequencies used to derive this exposure value and the values assigned to assets affected by these two major vulnerabilities. Once this process has been accomplished, countermeasures can be selected based on the recommended list of countermeasures. The asset exposure would then be completed again as needed until a suitable set of countermeasures was identified.

Threat Evaluation Form

THREAT NAME	THREAT FREQUENCY	
	RATING	PRECISION
Uncleared Personnel Access	4 (TABLE _-1)	F (TABLE _-2)

DESCRIPTION

Uncleared personnel, e.g., visitors, maintenance staff, or customer engineers, may be allowed unescorted access or greater access than warranted.

EXAMPLES & EVALUATION GUIDANCE

- Visitors who are part of an escorted tour may become separated from the group and enjoy unescorted access to vital elements of the ADP facility such as the tape library
- Frequent visitors to the ADP facility may be allowed to escort themselves to their destinations, thus bypassing the access control and escort procedures for visitors
- Visitors may observe classified information being processed
- Visitors may observe vulnerabilities in the ADP countermeasures for the purpose of exploiting these vulnerabilities; for example, they may observe staffing of guard stations at shift change
- Visitors may plant passive devices such as hidden microphones or active devices such as bombs
- Maintenance staff and customer engineers may not be properly escorted and supervised
- Unescorted persons may commit acts of vandalism

EVALUATION GUIDANCE

Estimate the probable frequency of attacks by uncleared personnel with legitimate access to the ADP facility. Sign-in logs can provide the number of persons admitted to the facility per year. The number of uncleared personnel who have greater access than warranted should also be considered. Using the total number of uncleared people as an upper limit, the risk assessor should estimate how many of these people may misuse their privileges or attempt to gain wider privileges.

IMPACT

DESTRUCTION ☒ DISCLOSURE ☒ MODIFICATION ☒ DENIAL OF SERVICE ☒

JUSTIFICATION

During the past year uncleared personnel gained access to the computer center four times. Figures for previous years are not available, but are believed to be about the same. Precision estimate of "fairly precise" is used since some, but not all, instances of uncleared personnel are detected and reported

Figure Att. _-1

THREAT TALLY SHEET

THREAT	FREQUENCY RATING	PRECISION
Post-Employment Access	4	R
Disgruntled Employee Access	3	R
Agent Access	2	R
Uncleared Personnel Access	4+	F
Emanations (Unintended)		
Emanations (Covert)		
Emanations (Interference)	1	R
Improper Marking		
Improper Handling		
Fraud	3+	R
Alteration of Software	3-	F
Alteration of Hardware		
Disclosure of Information		
Physical Theft		
Eavesdropping		
Misuse of Resources		
Intentional Denial (Software)		
Intentional Denial (Hardware)		
Power Instability	4	V
Telecommunications Failure		
Environmental Control Failure		
Sabotage		
Weather Damage		

Figure Att. _-2 (Page 1 of 2)

THREAT TALLY SHEET (Continued)

THREAT	FREQUENCY RATING	PRECISION
Natural Disaster		
Water Damage (Internal)		
Water Damage (External)		
Fire (Internal)		
Fire (External)		
Enemy Overrun		

Figure Att. _-2 (Page 2 of 2)

Vulnerability Evaluation Form

VULNERABILITY NAME	VULNERABILITY LEVEL
Application Software	HIGH (TABLE __-3)

DESCRIPTION

The application software may contain design or implementation flaws that could lead to a compromise of security.

EXAMPLES & EVALUATION GUIDANCE

- o Improper Marking. The application software may not properly mark classified or sensitive computer-produced information.
- o Imbedded Information. The application software may contain imbedded passwords or other sensitive information. This information could be disclosed inadvertently or perhaps not marked properly.
- o Error Handling. Application software which is designed to handle errors can often cause unwanted disclosures and possible denials of service.

EVALUATION GUIDANCE

The rating should consider the likelihood that application programs contain faults that could either disclose or destroy information or cause denial of service. Only programs that have legitimate access to classified data need be evaluated for flaws that could lead to disclosure. Application programs can cause denial of service in a number of ways; for example:

- o Excessive service requests
- o Failure to perform
- o Infinite looping
- o Crashing the system

Vulnerability will be greater if persons in a position to benefit from flaws have the opportunity to insert them. The rating should be based on how common the flaws are likely to be and how damaging the consequences of these flaws could be. Historical information can be used.

Unless certification of applications software has been done, the rating will be no lower than medium.

Consult the individual applications managers.

JUSTIFICATION

Numerous instances have been recorded in which unauthorized changes of a non-malicious nature have been made. These changes have destroyed the integrity of important data bases.

Figure Att. _-3

VULNERABILITY TALLY SHEET

VULNERABILITY	VULNERABILITY LEVEL
Covert Operating System Modifications	MEDIUM
Operating System Flaws (Unintentional)	MEDIUM
Application Software	HIGH
Communication Software	LOW
Inadequate Audit and Security Mechanisms	HIGH
Inadequate Error Detection	VERY LOW
Inadequate Protection Features	VERY LOW
Power Supply	HIGH
Environmental Support Systems	MEDIUM
Building Construction	LOW
Internal Physical Access Control	LOW
External Physical Access Control	MEDIUM
Inadequate Fire Protection	
Operations Procedures	
Software Development Procedures	
Software Acceptance Procedures	
Software Maintenance Procedures	
Input/Output Procedures	
Supply and Service Procedures	
Emergency Procedures	
Security Procedures and Security Office	
Management	
Personnel	

Figure Att. _-4 (Page 1 of 2)

Vulnerability Tally Sheet (Continued)

VULNERABILITY	VULNERABILITY LEVEL
Inadequately Protected Communication Links	
Communication Architecture	

Figure Att. _-4 (Page 2 of 2)

THREAT/VULNERABILITY MERGER FORM—MODIFICATION

THREAT FREQUENCY RATING / VULNERABILITY LEVEL		Post-Employment Access	Disgruntled Employee	Agent Access	Uncleared Personnel Access	Emanations (Interference)	Fraud	Alteration of ADP System Software	Power Instability		
		4	3	2	4+	1	3+	3-	4		
Covert Operating System Modifications	M		2				2				
Operating System Flaws	M		2				2	2			
Application Software	H		3-				3				
Communication Software	L						1+				
Inadequate Audit and Security Mechanisms	H		3-				3	2+			
Inadequate Error Detection	VL					0			0		
Inadequate Protection Features	VL							0			
Power Supply	H								4-		
Environmental Support Systems	M										
Building Construction	L					0					
Internal Physical Access Control	L	2-		1-	2-						
External Physical Access Control	M	2-		1	2-						
Fire Protection											
Operations Procedures											
Software Development Procedures											
Software Acceptance Procedures											
Software Maintenance Procedures											
Input/Output Procedures											
Supply and Service Procedures											
Emergency Procedures											
Security Procedures and Security Officer											
Management											
Personnel											
Inadequately Protected Communications Links											
Communication Architecture											

Figure Att. _-5

ASSET EVALUATION FORM

ASSET NAME	UNAUTHORIZED DESTRUCTION	UNAUTHORIZED DISCLOSURE	UNAUTHORIZED MODIFICATION	UNAUTHORIZED DENIAL OF SERVICE
ON-LINE DATA BASE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☒ YES ☐ NO 4 VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
PAYROLL PROGRAM	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☒ YES ☐ NO 6 VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
CENTRAL PROCESSOR	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☒ YES ☐ NO 5+ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
AUDIT RECORDS	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☒ YES ☐ NO 4+ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
O.S. SOFTWARE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☒ YES ☐ NO 5- VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE
	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE	DOLLAR VALUED? ☐ YES ☐ NO ____ VALUE

Figure Att. _-6

IMPACT CATEGORY: MODIFICATION
ASSET TYPE: DOLLAR-VALUED

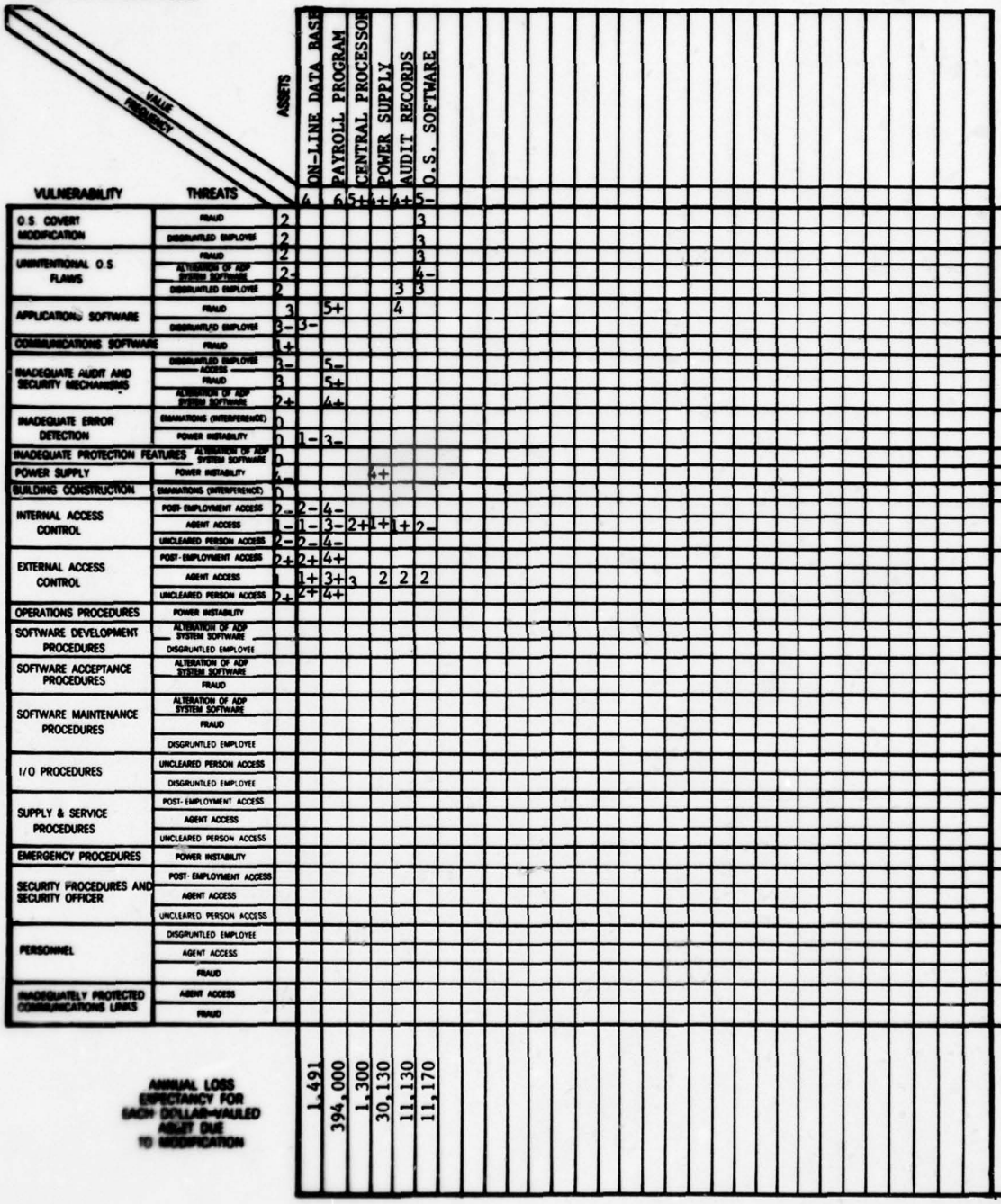


FIGURE ATT. _-7

ATT. _-12

TOTAL EXPOSURE FORM

(MODIFICATION ONLY FOR DOLLAR-VALUED ASSETS)

VULNERABILITY	TOTAL ANNUAL COST DUE TO VULNERABILITY
Covert Operating System Modifications	$ 2,000.
Operatng System Flaws	11,000.
Application Software	310,700.
Communication Software	0.
Inadequate Auditors Security Mechanisms	400,000.
Inadequate Error Detection	707.
Inadequate Protection Features	0.
Power Supply	30,000.
Environmental Support Systems	
Building Construction	0.
Internal Access Control	15,277.
External Access Control	64,930.
Fire Protection	
Operations Procedures	
Software Development Procedures	
Software Acceptance Procedures	
Software Maintenance Procedures	
Input/Output Procedures	
Supply and Service Procedures	
Emergency Procedures	
Security Procedures and Security Office Management	

Figure Att._-8. (Page 1 of 2)

Total Exposure Form (Continued)

VULNERABILITY	TOTAL ANNUAL COST DUE TO VULNERABILITY
Personnel	
Inadequately Protected Communication Links	
Communication Architecture	

TOTAL SYSTEM-WIDE ANNUAL LOSS EXPECTANCY

$834,614.

Figure Att. _-8 (Page 2 of 2)